United States
Department of State

Diplomacy in the 21st Century

Information Technology Strategic Plan

FY2001 – FY2005

January 2000

This .PDF file was created from the FINAL version of the IT Strategic Plan. Some images in that document did not convert to this format. We are working to rectify this problem.

United States
Department of State

Diplomacy in the 21st Century

Information Technology
Strategic Plan

FY2001 - FY2005

January 2000

Prepared by:

Office of Deputy Chief Information Officer
for Architecture, Planning, and Regulations
IRM/APR/IAP
2401 E Street N.W.
SA1 H334
Washington, DC, 20522

Message from the Under Secretary

Picture of the Under Secretary

I am pleased to issue the Department of State's new Information Technology (IT) Strategic Plan. This Plan presents the strategic IT goals we must attain to be successful in the 21st Century. It identifies new tools and capabilities that all members of the international affairs community will need to achieve U.S. diplomatic readiness around the world. The Plan is fully consistent with Secretary's priorities for diplomatic readiness.

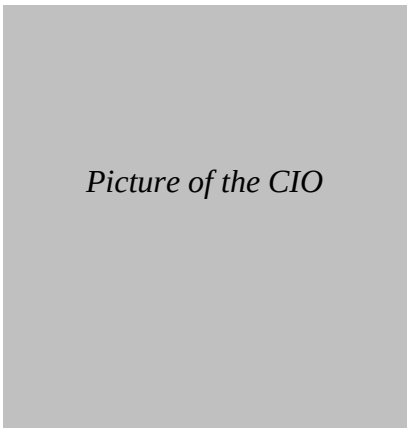
Although this Plan builds on our highly successful IT modernization and Year 2000 efforts, it also moves us toward a radical vision of the future – one in which our worldwide resources are linked together in an electronic global village. Capitalizing on the capabilities available in the commercial sector -- electronic commerce, the Internet, instantaneous high-speed communications -- we will create an electronic environment that effectively supports the pursuit of our diplomatic interests and priorities.

This Plan is totally consistent with our international affairs priorities in three important respects. It emphasizes support for the broad range of diplomatic, consular, and analytical activities that are at the core of the Department's mission. It calls for the establishment of a high-speed, secure, global communications network and IT infrastructure that will link all agencies that operate overseas, enabling us to collaborate efficiently to promote our national interests. Finally, it promotes careful risk management processes as the means for achieving high levels of IT security.

The Department must be ready for the challenges of the new millennium, and this Plan points us to the IT capabilities needed to meet those challenges. The entire Department must work together to focus its IT efforts and resources in support of this Plan, and I will be working with the Secretary to help bring this about. Therefore, I urge all of you to examine this document carefully and identify opportunities to work with the IRM Bureau to ensure successful accomplishment of this Plan's goals and objectives. I plan to work with OMB and the Congress to secure the necessary resources to make the bold vision presented in the Plan a reality. The Secretary and I are committed to providing the resources required to support diplomatic readiness around the world, and this IT Strategic Plan is among our highest priorities.

Bonnie Cohen
Under Secretary for Management

Message from the CIO



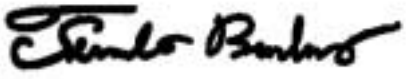
As we enter the 21st Century, the Department of State is facing unprecedented change in the conduct of international relations and at the same time is experiencing tremendous changes in Information Technology (IT). Today's conduct of foreign affairs requires that we be able to work closely with other US Government agencies, international institutions, host governments, and non-government organizations. If we are to advance our national interests successfully, we must be positioned to exploit the expansive access, speed, and analytical capabilities that information technology and rapid communications now afford. The leadership role of the United States in international affairs demands that we develop a fully responsive, yet secure, IT capability, including systems and tools that enable our employees to access, manipulate, and share up-to-date information and to collaborate with others in addressing foreign policy issues.

In addition, we must continue to streamline our operations, improving staff skills and exploiting information technology to make the Department more efficient and effective. We must modernize and revamp our most outmoded systems, including the cable system that has long served us well, deploying modern business-quality solutions. We must rely as much as possible on commercial technology and services, ensuring the flexibility and capacity to address new and changing requirements.

This new IT Strategic Plan positions the Department to meet the challenges of diplomacy that we will face in the new millennium. The Plan elaborates on the five broad goals adopted in 1998 in the "Goals 2005" paper, and builds on recent successes such as the worldwide, unclassified ALMA deployment. While it capitalizes on past successes, the Plan also presents a visionary blueprint for the future -- one in which our staff, wherever they are located, will have immediate access to the information, tools, and services needed for the conduct of *e-Diplomacy* in the information age.

This Plan was developed initially in draft form by the Bureau of Information Resource Management (IRM) with input from other bureaus, and then reviewed with all Department organizations. Bureau feedback was very positive and indicated broad consensus and support for the vision, goals, objectives, and strategies. Reflecting this broad support, the Information Technology Program Board has approved the Plan and intends to use it as a basis for investment decisions for IT projects. The Plan will provide a framework through which IRM and the Bureaus can work together to achieve the five goals the Department has adopted.

I am pleased to present this IT Strategic Plan and am convinced that achieving the goals presented in this Plan and moving toward a robust *e-Diplomacy* environment will position the Department well for the diplomatic challenges ahead.



Fernando Burbano
Chief Information Office

Table of Contents

EXECUTIVE SUMMARY

The Department of State has primary responsibility for the conduct of foreign affairs for the United States. It maintains embassies, consulates, and other facilities at more than 230 locations around the globe. It provides support for the overseas operations of all U.S. Government (USG) agencies represented abroad. In short, the Department is responsible for maintaining a state of *diplomatic readiness* to enable effective and efficient pursuit of U.S. global interests and priorities.

This Information Technology (IT) Strategic Plan presents the Department's plans for supporting the international affairs and diplomatic mission with modern, robust, secure, and cost-effective IT solutions. This Plan builds on recent modernization efforts that have gone a long way toward bringing the Department's IT environment into the 1990s – with this new Strategic Plan we are poised for the new millennium. This Plan provides a blueprint for prudent investments beginning in Fiscal Year (FY) 2000 and proceeding through FY 2005. The Plan will enable the Department to capitalize on advances in technology available in the private sector.

This Plan will position the Department to provide a common information platform at overseas locations to bring the benefits of e-diplomacy to all agencies operating overseas. The Overseas Presence Advisory Panel (OPAP) has issued draft recommendations calling for State to assume responsibility for extending this robust, standardized IT infrastructure to support the entire international affairs community. This Plan supports the OPAP recommendations fully and will promote effective exchange of information and collaborative processing among the multiple agencies with overseas presence.

While this Plan is a logical extension of past modernization and planning efforts, it also provides a radical and visionary blueprint for the future. Successful accomplishment of the Plan's strategic goals and objectives will require major changes in the Department's culture; the ways people carry out their responsibilities, and the supporting IT infrastructure and systems. The text box on the following page highlights key changes envisioned by this Plan.

Vision

The Plan is grounded in the concept of ***e-Diplomacy*** – the analog of electronic business in support of the conduct of international affairs and global diplomatic operations. The explosion in technologies such as the Internet, along with powerful data mining solutions, will enable the Department to revolutionize IT support for the mission-related activities of diplomacy, consular affairs, operations and management. This Plan will also unify IT support to all agencies operating overseas, if the Congress funds the recommendations in the 1999 OPAP Report, ensuring the ability to communicate, collaborate, and share information across varying types of platforms.

Successful accomplishment of the Plan's strategic goals and objectives will require major changes in the Department's culture, how people carry out their responsibilities, and the supporting IT infrastructure and systems

By 2005 State's IT environment will be radically enhanced with:

- A **centrally funded, deployed, and operated infrastructure** that ensures universal consistent, high-capacity and high-performance networks, platforms, and servers
- A **Web-based** environment that translates the capabilities of the Internet and electronic commerce into ***e-Diplomacy***
- **Replacement of the current cable system** with an integrated suite of off-the-shelf products for informal and formal messaging, for exchange of information of all types, and for centralization of formal messaging
- **Consolidated and centralized servers and databases** to realize the concept of the "data-less" Post – substantially reducing security risks and far-flung technical support requirements
- Significant investment in **desktop tools for the Department's employees** – supporting knowledge management through ready access to information sources, facilities for collaborative processing and team-work, and effective document management and retrieval
- Reliance on **commercial networking services** for all communications

Inexpensive, broadband global communications are indeed turning the world into a global village, bringing people and organizations together in ways that seemed impossible a few years ago. The Department's knowledge workers must be in a position to take advantage of the IT and communications revolution – they must be able to communicate rapidly with one another and with colleagues and peers in other U.S. and foreign government organizations, as well as with non-government organizations (NGOs) and the public. They must have access to a wide range of up-to-the-minute information sources, and the tools with which to identify, analyze, and present information to support policy formulation and execution.

The use of IT at State over the next few years will be based on two key concepts:

(1) ***Virtual teaming*** – through networks and software solutions, people will be able to participate in virtual teams to focus on both foreign policy and administrative issues. Physical location will be irrelevant for many activities, as video teleconferencing and similar techniques become widely used. This concept, coupled with a focus on knowledge management, will ensure that the Department's knowledge workers have quick and full access to the information needed to perform their mission regardless of the physical location of the people, the computers, or the information.

(2) ***User empowerment*** – many operational and administrative processes, such as human resources and procurement, can be highly automated and standardized – enabling self-service for many functions. For example, staff will be able to update most of their personnel information either online, via the web, or by telephone, much as people today do their banking and stock trading electronically. Support will also increase for mobile computing, portable solutions, and

flexible user-oriented technologies that mimic commercial environments. Integration, standardization, and commercial solutions will be keys to success.

The vision of the future is based heavily on commercial sources and technologies. Consistent with security requirements and Presidential Decision Directive 63 (PDD-63), the Department will take advantage of commercial advances and successes, rather than building its own infrastructure and IT solutions. The IRM Bureau will work closely with the Bureau of Diplomatic Security (DS) and other agencies in continual assessment and management of security risks, threats, and solutions.

Goals and Objectives

To achieve its IT vision, the Department will pursue five broad goals and thirteen strategic objectives. These goals and objectives, summarized in the table below, provide a focus for managing IT investments and setting priorities. A critical path model of these strategic objectives and supporting initiatives will shape the ongoing tactical planning and oversight of specific IT projects and investments.

Goal	Strategic Objectives
Goal 1: A Secure Global Network and Infrastructure	➢ Objective 1A - A Commercial-Style Global Network for Classified and Unclassified Communication ➢ Objective 1B - A Continually Updated Equipment and Software Base ➢ Objective 1C - Robust Infrastructure Security Services ➢ Objective 1D - Effective Infrastructure Management and Support Services
Goal 2: Ready Access to International Affairs Applications and Information	➢ Objective 2A - Worldwide Access to International Affairs Information Resources ➢ Objective 2B - IT Support for Effective Collaboration ➢ Objective 2C - Effective IT for Public Diplomacy
Goal 3: Integrated Messaging – A Modern Worldwide Approach	➢ Objective 3A - Business Quality Electronic Mail ➢ Objective 3B - Standard Utilities and Services for Information Exchange
Goal 4: Leveraging IT To Streamline Operations	➢ Objective 4A - User-empowered Administrative Systems ➢ Objective 4B - Consolidation of Information Technology Facilities
Goal 5: Sustaining a Trained Productive Workforce	➢ Objective 5A - A Rewarding Workplace for IT Specialists ➢ Objective 5B - An Effective Distance Learning Program

Strategic IT Goals and Objectives

Strategies

The Department will pursue the following broad strategies to achieve its strategic IT goals and objectives:

- ***Management Strategies*** – rigorous capital planning to align investments and projects with this Plan; careful yet rapid studies to set project direction, process improvement methods to re-engineer and streamline procedures in conjunction with automation; active management oversight and review; application of risk management principles, rather than risk avoidance, to address security requirements; liberal use of outsourcing whenever it makes sense to do so to take advantage of the expertise of the private sector; and the allocation of a majority of the resources in the Department's Central Fund (CF) to projects that directly support implementation of this Strategic Plan.

- ***Technical Strategies*** – a focus on exploiting the worldwide web and the Internet; broad and scalable connectivity, along with an easy-to-use front-end for user access through a standard browser; use of standards to ensure scalability and flexibility; enhanced technical project management and oversight, ensuring conformance with IT architecture and standards; rigorous quality assurance and configuration management (CM), independent verification and validation (IV&V); and pilot-testing of solutions in live post environments.

Resources

The Department's long-term goal is to provide the best possible IT support to mission critical diplomatic, consular, and management operations. At the same time, we are strongly committed to achieving efficiencies and controlling the ever-increasing share of our budget that must be devoted to IT. The Department has demonstrated its ability to meet its IT commitments efficiently and effectively. Examples are the highly successful programs to modernize our unclassified infrastructure overseas through A Logical Modernization Approach - ALMA, and to achieve Year 2000 (Y2K) compliance for our mission-critical systems. Through this Plan we will continue to enhance and improve our overall IT posture. International affairs is highly IT-intensive and dependent on necessarily costly systems – such as global networks and systems, highly specialized security solutions, and necessary redundancies to ensure reliability and support for contingencies. That notwithstanding, the Department believes that through this Strategic Plan, we will realize cost savings in specific areas, particularly in the out-years of the Plan. The Department is committed to lowering its total cost of ownership (TCO) enterprise-wide.

In the first two to three years of the next century, significant investments will be required to pursue the aims of this Plan. Investments will be required in a robust, commercial-style network, a security and messaging infrastructure, interagency connectivity as recommended in the recent OPAP Report, centralized facilities and services for enterprise IT management, web-based processing on modernized mainframes and other platforms, and streamlined applications and databases to support substantive and management activities. We will also invest in our vital human resources, spending considerable sums on recruiting, retention, and training. These investments will have a commensurate payoff – in enhanced mission effectiveness and diplomatic readiness, as well as efficiencies and cost savings in selected IT and operational areas.

INTRODUCTION

This document is the successor to the Department of State's IRM Strategic and Performance Measurement Plan, issued on January 15, 1997. Since issuance of the 1997 plan, the Department has made much progress with its Information Technology (IT) program. It has completed Year 2000 (Y2K) corrections to all of its mission-critical systems. It has published an Information Technology Architecture. It has installed up-to-date computer equipment at all of its 270 Foreign Service posts. It has provided secure Internet e-mail access to most of its employees. It has successfully implemented an IT Capital Planning process. And with the support of the Congress, it has built a Capital Investment Fund (CIF) that can help sustain the Department's IT progress for years to come. Appendix B provides additional details regarding accomplishments the Department has made on the IT initiatives set forth in the 1997 Strategic Plan.

Even as the Department's IT program progresses toward previously established objectives; it faces new challenges that require the setting of new objectives. The most obvious of these challenges is the recently completed foreign affairs agency consolidation, which will eventually result in the full integration of the IT systems of the Department, the Arms Control and Disarmament Agency (ACDA), and the United States Information Agency (USIA). To carry this challenge further, a report recently published by the Overseas Presence Advisory Panel (OPAP) recommends that State take the lead in ensuring connectivity and interoperability among all agencies operating overseas.

However, an even more fundamental shift in the Department's mission has arisen from new requirements for conducting diplomacy in the information age. The implications of this shift have been set forth in two recent independent reports by the Stimson Center and the Center for Strategic and International Studies (CSIS), along with the Department's own document, Diplomacy for the 21st Century: IT Goals for the First Five Years (referred to hereafter as the IT Goals Paper).

This is an ideal time for the Department to update its IT Strategic Plan. The Plan can build on the substantial progress already made in achieving previously-set objectives, while positioning the Department to face the new challenges that have arisen.

This document elaborates on the Department's strategic IT goals, originally described in the IT Goals Paper. The chapter immediately following this Introduction summarizes the Department's overall mission and strategic goals. A chapter setting forth the

Department's IT vision for 2005 follows it. The next chapter, which is the heart of this Plan, translates the five strategic IT goals in the IT Goals Paper into 13 strategic objectives, specifies the major milestones to be achieved under each objective, and identifies the performance measures to be used to evaluate results. The following three chapters describe, respectively, the strategies the Department plans to follow in achieving its IT objectives, the IT management and planning process that will ensure this Plan is carried out effectively, and the relative priorities the Department has set for its strategic IT goals. The final chapter discusses the cost impact of implementing this Strategic Plan.

This Plan focuses entirely on the future of IT in the Department. Readers who are interested in learning about the current IT environment should review the most recent IT Tactical Plan, which is published about every six months.

DEPARTMENT MISSION AND STRATEGIC GOALS

The U.S. Department of State Strategic Plan of 1997 includes the following mission statement:

"U.S. diplomacy is an instrument of power, essential for maintaining effective international relationships, and a principal means through which the United States defends its interests, responds to crises, and achieves its international goals. The Department of State is the lead institution for the conduct of American diplomacy. A mission based on the role of the Secretary of State as the President's principal foreign policy advisor.

In order to carry out U.S. foreign policy at home and abroad, the Department of State:

- Exercises policy leadership, broad interagency coordination, and management of resource allocation for the conduct of foreign relations;
- Leads representation of the United States overseas and advocates U.S. policies to foreign governments and international organizations;
- Coordinates, and provides support for, the international activities of U.S. agencies, official visits, and other diplomatic missions;
- Conducts negotiations, concludes agreements, and supports U.S. participation in international negotiations of all types;
- Coordinates and manages the U.S. Government response to international crises of all types;
- Carries out public affairs and public diplomacy;
- Reports on and analyzes international issues of importance to the U.S. Government;
- Assists U.S. business;
- Protects and assists U.S. citizens living or traveling abroad;
- Adjudicates immigrant and non-immigrant visas to enhance U.S. border security;
- Manages those international affairs programs and operations for which State has statutory responsibility; and
- Guarantees the Diplomatic Readiness of the U.S. Government."

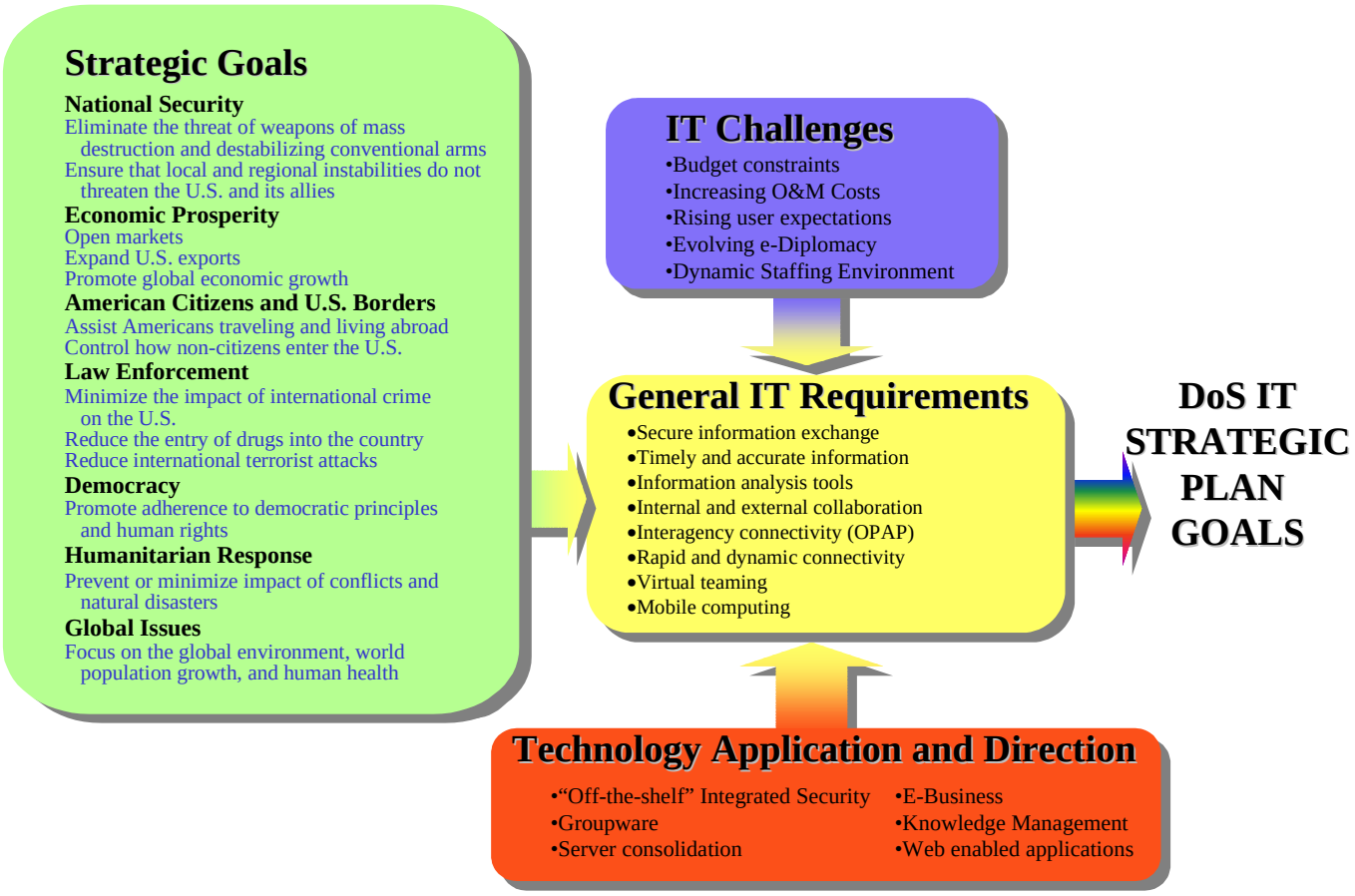
The Department's 1997 Strategic Plan identifies the strategic goals summarized in the table below:

AREA OF FOCUS	GOALS
National Security 	• Ensure that local and regional instabilities do not threaten the U.S. and its allies • Eliminate the threat of weapons of mass destruction and destabilizing conventional arms
Economic Prosperity 	• Open markets • Expand U.S. exports • Promote global economic growth
American Citizens and U.S. Borders 	• Assist Americans traveling and living abroad • Control how non-citizens enter the U.S.
Law Enforcement 	• Minimize the impact of international crime on the U.S. • Reduce the entry of drugs into the country • Reduce international terrorist attacks
Democracy 	• Promote adherence to democratic principles and human rights
Humanitarian Response 	• Prevent or minimize impact of conflicts and natural disasters
Global Issues 	• Focus on the global environment, world population growth, and human health

"New technologies, the communications revolution, and economic growth have increased the rate of global change and diminished the importance of time and distance. As a result, the world is more interdependent, while the consequences of political, economic, and military developments are more interrelated."

U.S. Department Of State Strategic Plan, 1997

As shown in the figure below, this IT Strategic Plan focuses on applying IT to support all of the strategic goals identified in the table above. The high-level IT requirements identified below respond directly to the Department's mission-oriented areas of focus and strategic goals. These requirements emphasize flexible, powerful information access, analysis, sharing, and collaboration among State knowledge workers, both internally and with external organizations, including other agencies operating overseas. The requirements also reflect commercial trends and directions in technology and IT management, such as knowledge management, web technologies, groupware, and security. Finally, the requirements recognize the major challenges and issues facing the Department as it moves into the next millennium, including budget constraints, staffing challenges, and rising user expectations.

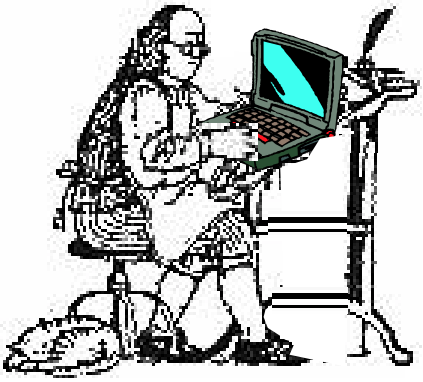


The next chapter projects an IT vision for 2005 that will help the Department accomplish its mission. This vision encompasses all of the elements shown in the above figure, linking directly to the mission goals from the Department's Strategic Plan.

This Page Intentionally Left Blank

IT VISION FOR 2005

The New Diplomacy



The Department of State stands on the threshold of a new era in the conduct of diplomacy. Issues facing our political and economic officers are increasingly complex, global, and intertwined. Much of diplomacy has become multilateral, with shifting alliances. Global issues, such as international terrorism, the environment, population, and refugees are becoming increasingly prominent, as evidenced by the Department's Strategic Plan. Diplomacy increasingly involves dealing with publics – both domestic and foreign, as well as with NGOs. People have rapid access to information about international events from many sources, and this colors their understanding and support for US foreign policy. The new diplomacy will have to deal with these changes.

Many US Government agencies operate overseas, interacting with each other and with State personnel. Our overseas IT infrastructure must accommodate these multiple agencies, creating an environment that promotes easy interagency connectivity and efficient IT support, as recommended by OPAP.

This new era in diplomacy will also be shaped increasingly by methods and approaches made possible by information technology. Advances in communications and computer technology, along with the explosive growth of the Internet, are already transforming the world into a global village. The Department must take steps to adapt its traditional methods of diplomacy to be effective in the new technological environment in which it now operates.

This is not to suggest that traditional diplomatic skills will be replaced by technology – far from it. The ability to formulate complex strategies, the ability to make nuanced judgments based on an understanding of the human condition, the ability to articulate positions precisely, the ability to respond appropriately to unexpected situations, the ability to persuade on the basis of trust painstakingly built up over a period of years – all of these abilities are, and will remain for the foreseeable future, human monopolies.

Nevertheless, diplomats must be well informed to be effective. They must be able to communicate rapidly and efficiently with partners and adversaries around the world. And they must have the infrastructure support that enables them to concentrate on their main business, rather than being constantly diverted by the demands of support activities. These are the areas in which technology promises to transform traditional diplomacy into ***e-diplomacy*** over the next decades.

By 2005 the Department of State will operate to a large degree through *e-diplomacy* – that is, it will apply the techniques of e-commerce to its diplomatic, consular, and management activities. Its employees will have ready access to internal and external databases that will keep them fully up-to-date on international events and the roles being played by all of the actors involved. They will have a variety of electronic ways to communicate rapidly and reliably with their colleagues and with members of other organizations, including host governments. And they will be able to devote more of their human resources to the Department's main business of diplomacy, rather than to routine administrative functions, however essential for diplomatic readiness the latter may be.

Trends that Drive e-diplomacy

Several key trends will characterize the environment of 2005 and will have a significant impact on Department of State operations and the supporting IT infrastructure. The most successful and admired organizations are already moving in the direction of these trends. Among the most important of these trends are:

- Globalization
- Virtuality
- Flexibility
- Collaboration
- Learning-orientation and knowledge management
- Competition

The table on the following page explores each of these trends in relation to the future of e-diplomacy and State's operational and IT environment of 2005. While we cannot be certain of how these trends will play out, this table and the discussion, which follows, provide a framework for a conceivable vision for 2005.

Trend / Characteristic	Description	Impact on State Operations	IT Requirements
Globalization	Rapid, reliable, secure communication will continue to make the world smaller, connecting people everywhere in a web of networks and information. Information will pass rapidly around the globe.	While State is of course already a global enterprise, the future will see the globalization of the work group and increased leveraging of staff and expertise, and all made possible by information technology.	• Secure, reliable, scalable global infrastructure - available on a 7-day. 24-hour basis • Internal networks intertwined with the Internet, with carefully managed boundaries • The best tools for data mining, analysis, and presentation
Virtuality	Enterprise assets, resources, and configurations will be fluid, with much use of outsourcing, temporary and specialized employees. Effective organizations will be highly focused on what they do best, partnering with other organizations for other services. Location will be increasingly irrelevant.	Virtual teams for crisis management, issue analysis, and country operations. Increased reliance on commercial services and outsourcing, and on centralization to allow each Bureau and post to concentrate on its core business. Focus on relationships with NGOs, commercial firms, and other nations. Post and organizational specialization and focus.	• Collaborative and interactive technologies • Availability of procurement options for rapid response • Centralized service offerings in IT operations and management • Highly automated administrative functions such as Human Resources (HR), logistics, and finance • Mobile and home-based computing
Flexibility	The pace of change will continue to accelerate, and nimble organizations will be the survivors.	Reduced reliance on rigid hierarchical organizations replaced by fluid teams formed as needed. Rapid update and communication of policies and procedures.	• Use of the global network and web as a vehicle for communication • IT support for team-work -- collaborative software, interactive video conferencing • Mobile computing
Collaboration	The complexity of the issues to be addressed demands collaboration among individuals and organizations.	State must organize itself to promote internal and external collaboration -- among posts, geographic and functional bureaus, and with NGOs, other agencies, other nations	• IT support for team-work -- collaborative software, interactive video conferencing • Online communities • Interagency connectivity • Secure, high capacity networks • Directory services

Trend / Characteristic	Description	Impact on State Operations	IT Requirements
Learning-orientation and knowledge management	Successful organizations recognize the value of continuous learning throughout the organization. The passion to acquire knowledge is a key value in keeping up with customer demands and the competition.	While State has a tradition of emphasizing learning -- e.g., the Foreign Service Institute (FSI), it must transform its approach to promote constant learning at all levels – not just while FSI but throughout one's career.	• Knowledge management • Distance learning • Structured access to information from all relevant sources • Online interaction with experts
Competition	Customers will have increased choices from among multiple sources -- for information, services, products, everything	State will face increasing competition from think tanks, NGOs, the media, the web -- its customers will demand better, more timely, more accurate information and analyses. State must adapt or risk marginalization.	• The best tools for access to and analysis of information relevant to international affairs • A robust, secure, continually evolving IT infrastructure

The IT Environment of 2005

The evolution of Information Technology will mirror these trends in many ways. By 2005, the use of the Internet will be pervasive – people will be able to access the web from virtually anywhere in a large variety of ways. All forms of communication will be increasingly integrated and seamless. We will be able to check e-mail and voice mail from home, or while travelling, and we will be able to use smaller and smaller devices. Access to technology will become easier and more user-oriented. Speech and handwriting will be much more common forms of data entry, and computers will be able to recognize natural language with great accuracy. Video, audio, images, voice, and all other forms of information will be routinely available through a single Transmission Control Protocol/Internet Protocol (TCP/IP) network. Security features will keep pace with demand, allowing electronic transactions for virtually all types of e-commerce, and high levels of protection for sensitive information and networks.

The table on the following page characterizes key changes in the Department's IT environment that will accompany the broader changes discussed above. In general, the environment of 2005 will emphasize knowledge management – information technology tools and databases that enable the Department to leverage its vast store of corporate knowledge, making it widely available to those who need it, whenever and wherever they need it. This is a radical improvement over today's largely fragmented information environment.

Department IT Characteristics	1999	2005
Access to information	• Limited	• Worldwide
Work processes	• Isolated • Dispersed • Bureaucratic	• Collaborative • Consolidated • Self-service
Internet usage	• Partial	• Pervasive
Messaging	• Cable-based • Slow/unreliable	• Integrated e-mail / cable / data / video • Fast / reliable
Applications	• Stovepipe • Administrative • Distributed Data	• Integrated • Substantive • "Data-less" Posts
Workforce	• IT users poorly trained in effective use of IT • IT knowledge of many technicians outdated	• IT users well trained in effective use of IT • IT knowledge of most technicians up-to-date

Future Directions

As the changes discussed above actually occur, the State Department will change its way of doing business in many respects. Obvious changes are that work will become increasingly automated, and online interaction among people will be a dominant part of the workplace. Subtler, yet equally important, changes will occur in organizational and interpersonal relationships. For example, as organizations become more "virtual", traditional hierarchies will lose their importance. People will have ready access to each other and to various kinds of knowledge and expertise, thus altering today's power relationships. The paragraphs below illustrate new ways of doing business and suggest how IT will affect State programs and operations.

The substantive work of the Department will be characterized by global **virtual teaming.** Using technological advances, the Department will be able to assemble teams of experts to focus on the key issues of the day – especially the national interests and priority areas from the Department's Strategic Plan. The members of these teams need not be co-located, and the composition of teams can be changed rapidly as the need for different expertise and perspectives changes. Members need not all be internal employees – outside experts, NGOs, other agencies, all can play roles. The environment will be dynamic and flexible, enabling far more rapid and comprehensive attention to key issues than is possible today. Interagency connectivity, as called for in the OPAP report, will be a key underpinning of *e-diplomacy*.

Diplomatic communications will change to correspond to this virtual teaming environment. No longer will people be content to communicate vital information via outmoded and inflexible cables. In the future, communication will be much like the web – it will be real-time,

interactive when needed, multi-media, and flexible in format and style. Materials under development by team members can be made readily available for real-time review and discussion – all via easy-to-use network facilities. People all around the world can contribute to a document, reviewing each other's work in ways that best suit their personal styles.

Self-service or autonomy will characterize the administrative work of the Department**.** Technology will empower employees to enter much of their own data and process their own transactions in such areas as personnel, travel, purchasing, budgeting, and financial reporting and management. Technology can eliminate the "middle-man", much as online booksellers have reduced people's dependence on traditional bookstores. With the right tools, it is faster, easier, and more pleasant to shop via the net. So it will be for many routine administrative transactions. Security features will ensure proper review and accountability.

A key focus for IT will be **knowledge management** – establishment of databases and tools to leverage the tremendous storehouse of data and information the Department creates, receives, or accesses. The information age has created information overload for many people, including Department of State employees. People are unable to process or absorb all the potentially relevant information available to them. Department employees are especially vulnerable to information overload, since they are so dependent on information for their daily work. Sophisticated tools are under development to help people access and manage information far more intelligently than is possible today. Profiling, search and retrieval, pattern recognition, data mining, and other techniques are coming into wide use. The Department's IT environment of the future will capitalize on these developments to provide the best support possible for its knowledge workers.

The paragraphs below indicate how IT may change the Department by 2005:

- ***The Post Environment of 2005*** – the post of the future will be staffed almost exclusively by substantive knowledge workers, focusing on the strategic issues of United States diplomacy and consular affairs. Most posts will have very few or no permanent administrative staff, with administrative activities performed via self-service using easily accessed central systems. The post IT and operating environment will be more highly integrated than it is today – all members of the country team, regardless of agency, will be able to communicate with one another via a standard network and will participate in the virtual teams discussed above. The post will also interact more frequently with other posts and with external organizations – via the Internet, video conferencing, and online communities of interest. Posts will also be physically smaller, as staff is able to work from home, accessing systems and networks via mobile and portable equipment, which will also be getting smaller and more effective. In selected cases, the Department will move toward "data-less posts"; in high threat areas, especially, data will be maintained centrally rather than at post. Access will be provided through networking facilities.

- ***Consular Operations*** – Consular officers will be connected in real time to their peers at other posts and to Headquarters, enabling effective sharing of information for border security and visa processing. Biometrics will be used extensively, and the Department will experiment with fully electronic travel documents much as the airlines have done. Information systems and databases will aid in providing the best and most informed citizen's services to Americans overseas.

- ***A Day in the Life of a Political Officer*** – while the political officer's day will be more dynamic and demanding in the future, information technology will enhance his or her ability to meet the demands. The volume of information will be potentially overwhelming, and State's officers will be expected to keep up. They will use sophisticated tools to search for and obtain the data they need. The Department will have established systems and tools to aid them in this effort – specialized end-user desktops or toolkits will be provided for political, economic, consular, and management officers. They will also spend much time in interactive work groups, working with peers at other locations and in other organizations, bringing their special expertise to bear on the problems of the day. They will no longer focus their energy working alone to produce rigidly formatted cables, but rather will be able to share and present information in a variety of effective formats and media – working in a team environment. Sophisticated modern technologies, such as today's personal data assistants (PDAs) will free people from their desktops and allow access to critical information and communication among team members regardless of location. The entire analytical process will be more flexible, dynamic, and interactive than it is today, resulting in higher quality products, and a more rewarding work environment.

- ***Crisis Management*** – in the future, crisis management will rely on the virtual teaming concept to bring together the needed expertise and information as rapidly as possible. Task Force members will be in constant communication with each other and with others who may play roles, both in and outside State. In addition, crisis management will benefit from the ready access to the myriad information sources, which will be available in 2005, including information on past crises and responses.

- ***Human Resources Management and other Administrative Operations*** - Through technology, people will be given **autonomy** to initiate and process most administrative transactions, with systems in place to ensure appropriateness and authority. Technologies we might expect to see include smart cards, debit and credit cards, interactive voice response systems, and other forms of fully integrated electronic commerce. Consider human resources. The most innovative companies have radically streamlined their HR operations; in the most extreme cases they provide virtually all services from a single central location staffed by a small number of people. The HR function has become largely "self-service" through automated tools, accessible by employees and managers via the web, telephone, and other convenient means. Not only has this reduced costs consid-

erably, it has improved service and quality by reducing bureaucratic obstacles. By 2005, State should be able to achieve a radical transformation of its HR and other administrative operations, seeking out the best practices of the most innovative enterprises. By pursuing the goal of self-service, State can streamline and improve all administrative operations. For example, staff will be able to initiate purchase transactions that will be routed automatically to the best path for purchase, taking advantage of available discounts, delivery options, and other terms.

Rapid movement toward e-diplomacy will require cultural changes in the Department of State. It will require employees to master technology as a means for becoming more productive and effective. It will require an increased level of "openness" by involving, rather then excluding, other organizations participating in international activities and, most importantly, engaging the U.S. public in meaningful colloquies. It will require the Department to re-balance the always-vexing equation between security and openness, and to do so in favor of the latter. And it will require a focus on applying technology to the Department's main business, rather than to the administrative support systems that have traditionally absorbed all available IT resources.

IT GOALS AND OBJECTIVES

The Department's five strategic IT goals for the 2001-2005 period were initially set forth in the IT Goals Paper. This section further describes these five goals, breaks them down into the 13 strategic objectives listed below, and establishes milestones and performance measures for each objective.

Goal 1 - A Secure Global Network and Infrastructure

Objective 1A - A Commercial-Style Global Network for Classified and Unclassified Communication

Objective 1B - A Continually Updated Equipment and Software Base

Objective 1C - Robust Infrastructure Security Services

Objective 1D - Effective Infrastructure Management and Support Services

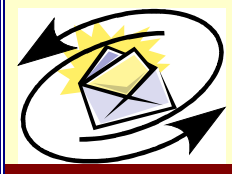
Goal 2 - Ready Access to International Affairs Applications and Information

Objective 2A - Worldwide Access to International Affairs Information Resources

Objective 2B - IT Support for Effective Collaboration

Objective 2C - Effective IT for Public Diplomacy

Goal 3 - Integrated Messaging – A Modern Worldwide Approach



Objective 3A - Business Quality Electronic Mail

Objective 3B - Standard Utilities and Services for Information Exchange

Goal 4 - Leveraging IT To Streamline Operations

Objective 4A - User-Empowered Administrative Systems

Objective 4B - Consolidation of Information Technology Facilities

Goal 5 - Sustaining a Trained Productive Workforce

Objective 5A - A Rewarding Workplace for IT Specialists

Objective 5B - An Effective Distance Learning Program

Goal 1 - A Secure Global Network and Infrastructure

A reliable and secure global telecommunications and processing infrastructure is the foundation for achieving all of the Department's strategic IT goals. The conduct of diplomacy and international affairs activities is increasingly dependent on information technology that is available at all times and all locations around the world, and that support modern information access and sharing. The Department's IT infrastructure must enable the nation's diplomats to exploit technology for innovative and collaborative processing and interaction, both internal and external.

***A modern, high-capacity, commercial-style network** is prerequisite to the conduct of e-diplomacy.*

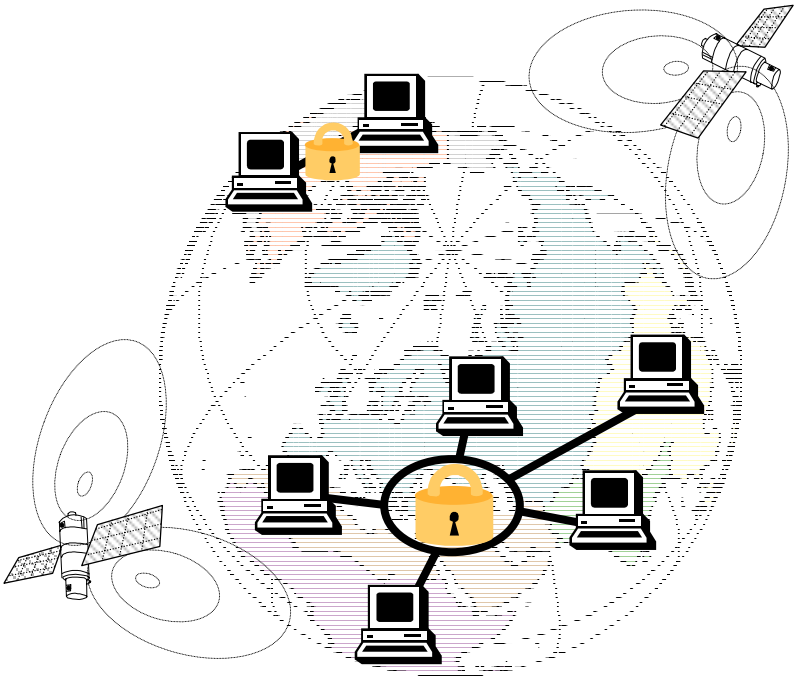
Global Reach

This first goal will focus on the establishment of a modern, scalable, commercial-style network and platforms for the diplomacy of the 21st century – an infrastructure with true global reach. End-users will connect to the infrastructure using a variety of modern devices – not just state-of-the-art desktop and laptop computers, but also telephones, televisions, voice input equipment, and other not-yet-invented devices. The infrastructure will provide the processing power, communications capabilities, security, and network management facilities needed to meet mission and business requirements and user expectations. Specifically, this goal will be achieved with establishment and maintenance of the most modern available computer and communications technology to support worldwide diplomatic, consular, and management activities.

Benefits to Diplomacy

Department employees will be able to use this network and technical infrastructure to:

- Communicate rapidly, securely, and reliably in a variety of conventional and innovative ways, including message text, voice, and video-conferencing;



No Longer A Luxury - Ubiquitous Global Communication Is Vital

- Communicate from desktop to desktop with each other and with others involved in foreign affairs activities – USG agencies, international organizations, NGOs, foreign governments, and U.S. firms engaged in foreign commercial activities;

*We must create an environment that **minimizes the complexities** inherent in globally dispersed IT systems.*

- Work collaboratively on foreign policy documents;
- Exchange textual materials, photographs, television images, data arrays, maps, engineering drawings, and biometrics, along with other forms of information;
- Gain rapid access to international affairs documents, information, and data; and
- Apply innovative technologies as they become available to support remote access and processing, wireless communication, integration of voice, data, and video information, and mobile computing and communications.

Two key characteristics of the IT environment of the future will be flexibility and sustainability. Flexibility is needed to keep the infrastructure reasonably current so that our Foreign Service officers and other knowledge workers are able to access the resources they need and communicate with their counterparts around the world. This goal promotes flexibility in a number of ways. First, it institutionalizes and expands the ALMA Program to promote regular, planned replacement and upgrading of IT assets. Second, the infrastructure will exploit commercial technologies and standards, rather than investing in proprietary solutions that cannot keep up with requirements and expectations. Third, this goal and the implementing strategies will encourage innovation, so that new technologies are evaluated in a timely manner and successful ones are incorporated and integrated rapidly into the infrastructure.

Sustainability is critical for the Department since it must maintain and support a far-flung infrastructure with diverse requirements and skill sets. A further challenge is that increasingly short-handed professional IT staffs supports this global infrastructure.

The infrastructure will be:

- ***Available, reliable, fault-tolerant** – everywhere when needed*
- ***Flexible and scalable** – to offer required capacity when needed – on demand*
- ***Secure** – protected from internal and external threats*
- ***Manageable** – supported by automated and integrated tools and services, along with a well-trained, skilled staff*
- ***Focused on supporting the end-user** – providing powerful and flexible access, supporting mobile computing, multimedia, and other such capabilities*

Objective 1A - A Commercial-Style Global Network for Classified and Unclassified Communication

The Department has long recognized that it must substantially improve its capability to add network capacity, increase availability, and adopt new services for the domestic and overseas environments. The current networking approach has been unable to keep up with demand or with the pace of change seen in commercial networking operations. State Department staff – including ambassadors – find themselves unable to communicate effectively among their country teams, between posts and Washington, or with external organizations. The Department's highly successful deployment of the ALMA platform has further demonstrated the need to upgrade circuit capacity at posts. To address this need, the Department has worked with the Diplomatic Telecommunications Service Project Office (DTS-PO), at considerable expense, to provide posts with additional bandwidth which in some cases became inadequate, even before the worldwide installation was complete. As the global telecommunications environment expands and blossoms, the Department must take greater advantage of commercial services to increase bandwidth capacity and drive down costs. This is the only way the DTS will keep pace with the communications demands of modern diplomacy.

Through this objective the Department will establish a robust, secure communications environment that supports Department mission and business requirements into the future. The Department will work to transform the DTS into a "utility" service that is always present, when demanded, to support sudden and short-term communications needs. Whether in Washington, at post, in travel status, or communicating outside of government, our diplomats will have immediate access to government-owned and contracted commercial services that, together, will constitute a secure, global, electronic highway for e-diplomacy.

Global Directory

Single authoritative source of directory (including applicable security information) on:

- ***People,***
- ***Organizations,***
- ***Functions,***
- ***Services, and***
- ***Documents.***

Accordingly, the major component of this objective is to position the Department to exploit available commercial

Current

The current networking approach will likely be ***prohibitively expensive and cannot deliver*** *the rapidly scalable capacity and services required.*

Future

The networking approach of the future will ***leverage the commercial sector's investment*** *in robust worldwide communications – meeting capacity and service requirements at affordable prices.*

technology and circuitry to the maximum extent possible, consistent with needs for availability and security. The aim is to establish a robust, scalable network that can support mission needs as they evolve and grow. Advances in hardware, software, and information management will place ever-greater demands on the DTS network, and the Department must be prepared to meet these demands. Whereas in the current dedicated circuit environment, upgrading bandwidth capacity is expensive and time-consuming, in the future, we must be able to provide a way to increase bandwidth on demand.

Virtual Private Network

Take advantage of the IP Security Protocol to ensure secure VPN transactions.

To capitalize on commercial networking technology, the Department plans to employ Virtual Private Network (VPN) services within the DTS. This will allow protection of sensitive information, while exploiting the tremendous bandwidth, throughput, cost-effectiveness, and other features of commercial circuits and services. Government and private sector organizations are beginning to deploy VPNs, and the technology is becoming ever more reliable, robust, and secure. The Department currently has six posts using VPN technology to provide access to Open Net via the Internet, and the experience at these posts will be used to plan further expansion in the use of VPNs within the DTS.

The network will continue to support all levels of classified and unclassified processing required by the international affairs community. The bulk of the processing is expected to be unclassified – either Sensitive But Unclassified (SBU) or totally unrestricted, with a smaller, although growing, percentage for classified processing (Confidential, Secret, and Top Secret). Under this objective, the Department will build, architect, deploy, and maintain network services meeting all of these requirements. This objective includes full Internet access, support for mobile computing, video conferencing, and, in general, the network underpinning for all the other goals and objectives.

The Department's network of the future will also include a standards-based global directory to support all

Implementation of commercial style networking will enhance our ability to perform the Department's mission by providing the following benefits:

- ***Increased and more timely internal and external interaction,*** *resulting in improved analyses, more thorough research and discussion of issues, and timely release of information to Department customers and the public;*
- ***Increased efficiency*** *through reduction in manual and paper-based processes;*
- ***Enhanced access*** *to sources of information through the Internet and other vehicles;*
- ***Increased reliability*** *of communications services, enhancing diplomatic readiness, embassy security, and emergency preparedness; and*
- ***Ability to constrain networking unit costs*** *(i.e., cost per unit of circuit capacity) by exploiting commercial networks such as the Internet.*

applications and end-user functions that require it. The directory will support electronic mail, modernized messaging, employee identification and authentication functions, as well as transaction routing, collaborative processing, and workflow applications. In keeping with the Federal interagency Public Key Infrastructure (PKI) and e-mail initiatives, a subset of directory information will be available for external access and communication.

Means and Strategies

Both short and long-term strategies will be used to build and sustain a robust global network needed for e-diplomacy. The following are the key strategies currently envisioned:

- ***Exploitation of commercial investments*** – the Department will make full use of the Internet, VPN technology, circuits provided by commercial carriers, satellite and other wireless systems, as appropriate, to provide a sustainable, scalable, reliable, and secure networking infrastructure. Consistent with security requirements, the Department will maximize use of these commercial technologies as a way to control costs while ensuring adequate and evolving service and capacity. The Department will proceed cautiously to implement global VPN services within the DTS, with a pilot deployed in 2001, and full-scale deployment to follow when the Department is convinced that this is prudent.

Ensure Readiness

1. ***Stop buying circuits – buy service***
2. ***Anticipate requirements and deliver capacity on demand.***

- ***Network consolidation*** – to promote effective network management and user productivity, the Department will collapse its networks to as few as possible. During FY 1999 and 2000 (that is, prior to the start of the planning horizon addressed by this Strategic Plan), the unclassified networks supporting SBU information and Internet access will be combined. An approach for this level of consolidation is currently being developed by the Office of Information Resources Management (IRM) and the Bureau of Diplomatic Security (DS). This consolidation will provide users with full access to the Internet from the same desktop they use for most Department processing. As security technologies advance and true multi-level security becomes available, access to classified information may also be provided from the same desktop. In any event, network management services (planning, monitoring, configuration management, user support) will be consolidated for all networks.

- ***Capacity planning and management and bandwidth on demand*** – the Department will establish an

enhanced process to monitor global capacity requirements, and ensure that required capacity is available when needed. This effort will be forward-looking, and will consider the impact of new technologies – e.g., video conferencing, voice over IP. The Department will work with DTS-PO to establish flexible and timely options for obtaining required communications capacity and services when needed.

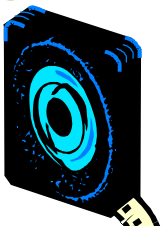
- ***Service Delivery Options*** – the Department and DTS-PO will explore various options for acquiring and delivering telecommunications and networking services. The goal is to provide the best possible networking services while reducing total cost of ownership (TCO). Available options include various forms of performance-based contracting, acquisition of services and bandwidth on a regional or global basis, and multiple award contracts, such as was used by the General Services Administration for FTS-2000. In 2001, the Department, in coordination with DTS-PO, will conduct a feasibility study and develop a comprehensive network plan. As the global commercial networking industry matures, the DTS must be positioned to take maximum advantage of the various options available for obtaining the very best and most cost-effective commercial services.

- ***Dedicated bandwidth for Command and Control requirements*** – recognizing the foreign affairs community's need for uninterruptible, secure, and highly reliable communications for mission critical requirements, the Department will continue to employ dedicated circuits (terrestrial and satellite) as its primary telecommunications medium in conjunction with newer commercial services such as VPN and on-demand bandwidth. Employing multiple service types will help to increase capacity and availability while driving down the unit cost of bandwidth. In this "meshed" network scenario, it is very possible that a majority of data will travel over VPN and on-demand circuits allowing DTS-PO to size the primary dedicated circuit to meet command and control requirements. Additionally, DTS-PO's customers will be able to choose the level of service they need for their data. For instance: a customer may choose only one path or choose to send a percentage of data over multiple paths.

Major Milestones

Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured



FY2001

- ⌂ Full Internet services available to all Open Net users
- ⌂ Study of network service delivery options
- ⌂ Global pilot test of commercial networking technology (e.g., VPN, Internet as transport mechanism)
- ⌂ Comprehensive plan for providing highly scalable circuit capacity on demand
- ⌂ Standards-based global directory established

Output
- Number of Department employees with full Internet capability

Outcome
- Evidence of innovative use of Department networks – e.g., for distance learning, video teleconferencing

FY2002

- ⌂ Comprehensive plan for command and control network, including support for highly classified communications
- ⌂ Establishment of bandwidth on demand for 50% of posts
- ⌂ Pilot test of voice over IP
- ⌂ Plan for integration of voice and data communications

Output
- High levels of network availability and reliability (e.g. greater than 99% availability)

Outcome
- Growth in use of networking services, collaborative interaction, web-based processing

FY2003

- ⌂ Pilot test of command and control network
- ⌂ Establishment of bandwidth on demand for all Department locations

Output
- Extent of use of commercial networking facilities
- Ability to meet demand for circuit capacity

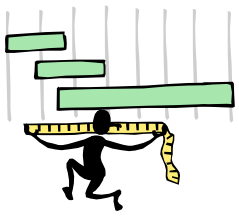
Outcome
- Post perceptions regarding network performance and capacity improve

FY2004

- ⌂ First increment of Command & Control network installed

FY2005

- ⌂ Command and control communications operating by satellite worldwide



External Factors

Achievement of this objective will require close cooperation with DTS-PO and all members of the international affairs community. The Government will benefit significantly from a coordinated global network that supports all international communications for all agencies. Attainment of some milestones is dependent on advances in networking and telecommunications capabilities and technologies (e.g., voice over IP and integration of voice and data).

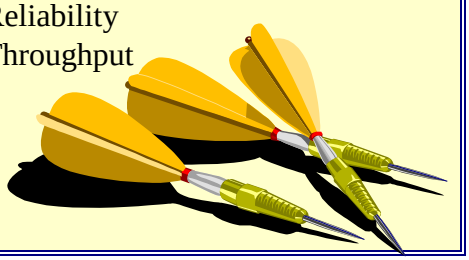
This objective calls for the use of commercial services and competitive practices to enable the high capacity, scalable, and secure global network needed for the diplomacy of the next millennium. The Department and DTS-PO's approach to networking must change dramatically – we must provide higher capacity, better service, and scalability, at affordable prices. More business-like arrangements, such as performance-based service level agreements (SLAs), will be established. These SLAs will be based on standard measures of network performance – that is, Delay, Availability, Reliability, and Throughput or DART – rather than the current focus on raw bandwidth.

The direction of the IT industry has always required ever increasing network capacity. Every new generation of software, such as word processing, e-mail, human resources, financial management, procurement, and other applications, offers new features and functions, but also requires increasing capacity for networking and processing power. The trend toward web-based applications typifies this. The Department must ensure that its network offers the necessary capacity to allow full use of these modern applications.

DART

Performance is measured in:

- Delay
- Availability
- Reliability
- Throughput



The Department will work with other agencies with overseas presence to coordinate the planning and development of the global network. As noted in the OPAP Report, interagency connectivity is a key underpinning of *e-diplomacy*. State will take the lead in ensuring effective levels of connectivity through an integrated networking approach.

Objective 1B - A Continually Updated Equipment and Software Base

The Department has made great strides in fielding modern platforms, especially the ALMA Program's deployment of unclassified systems at overseas locations and the modernization of mainframe technology at Beltsville and Main State. Among the benefits realized from these efforts are availability of modern hardware and software environments that support user requirements and expectations, as well as high levels of standardization and consistency, which have eased burdens on both end-users and the support infrastructure. Interoperability and data sharing have increased as end-users are able to exchange information using standard hardware and software.

But these successes also demonstrate how much more remains to be done to institutionalize a process for keeping technology aligned with State requirements. The Department will take an enterprise life cycle approach to platform management. Initially, the ALMA Program had been applied only to the overseas unclassified environment, leaving unmet the requirements for a modernized classified environment, as well as gaps in the domestic infrastructure. Bureaus have been inconsistent in their planning and spending for regular equipment upgrades and replacement. If this continues into the future, it will be impossible to maintain a substantially standardized environment. Excessive enthusiasm for decentralization has resulted in a proliferation of servers, bringing unacceptable levels of complexity, increasing costs and risks.

The Department has only just begun to exploit web technology, and this effort will be expanded and institutionalized under this strategic objective. The Department's growing dependence on web technology will inevitably increase its demands for a powerful server infrastructure accessible from anywhere in the world.

Life Cycle Replacement

Life cycle replacement results in flexibility to:

1) Capitalize on industry directions,
2) Manage total cost of ownership,
3) Avoid proprietary lock-ins, and
4) Attract and retain first-rate technical staff.

*A life cycle replacement program is **key to diplomatic readiness** – plus it enables us to attract quality technical staff and to capitalize on industry direction.*

Means and Strategies

The Department will build on the successes noted above and pursue three inter-related strategies to achieve this objective.

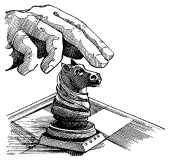
Investment Management through the Central Fund

Historically, planning and funding for IT hardware and software have been left to the individual Bureaus. The Bureaus are thus forced to choose among programmatic, administrative, and IT initiatives, when allocating their funds. The result is that each Bureau determines whether and when to replace or upgrade IT hardware and software. Over a very short period of time, this leads to a non-standard environment, which in turn reduces opportunities for information sharing and increases the training and support burden.

*The Department will use the **Central Fund** to promote effective life cycle management of hardware and software.*

To address this situation, the Department will expand the use of its Central Fund (CF) to cover ongoing maintenance, upgrade, and replacement of standard hardware and software suites. This is the only way to establish an effective life cycle maintenance program that sustains a reasonably standardized and interoperable environment.

Each year, the Department will establish an integrated plan for hardware and software funding. This plan will be coordinated with the IRM planning and architecture processes, which will continually identify hardware and software technologies and standards to be pursued. Each item of hardware and software will be assigned an expected life cycle (e.g., four years for desktop computers), and the annual plans will identify the specific items to be replaced each year.



Institutionalization of Key Programs and Initiatives

The IRM Bureau will establish an ongoing deployment program, building on the recent successful ALMA deployment. The expanded and ongoing ALMA process will address requirements for classified processing, and will ensure regular life cycle replacement and management of deployed platforms. The ongoing ALMA process will also work with any domestic Department organizations that require assistance in keeping current with desktops, servers, and other distributed processing platforms that come available. The ALMA program will continue to deploy and upgrade the Department's standard software suite.

The Department will continue its mainframe modernization process, systematically replacing all older-style processors with modern, Complimentary Metal Oxide Semiconductor (CMOS)-based equipment and instituting parallel sysplex to provide the reliability, avail-

*Modern mainframes will be used as **corporate super servers** for web services.*

ability, and scalability required for border security and other mission-critical initiatives. These modern mainframes will also be used as corporate servers to provide global processing support for corporate applications and data. This will allow continuing consolidation and centralization of processing onto fewer large-scale servers that are easier to manage, secure, and maintain than a host of disparate, widely dispersed servers. Web-based applications and data management will be encouraged, as a means of creating both broad-based access from anywhere around the world and easier–to-maintain systems. Centralized corporate platforms will be configured to provide the ideal environment for these web-based systems. These platforms will provide the reliability, performance, capacity, and scalability needed for the processing demands of the next century.

Procurement Strategies

The rapidly changing IT industry demands flexible and responsive procurement mechanisms. Department organizations must be able to purchase the latest technology – consistent with architectures and standards – easily, rapidly, and at commercial prices. The Department will create an online IT purchasing process that intelligently aids the purchaser in identifying the best vehicle for purchasing any given item.

This automated procurement environment will exploit Government-wide contract mechanisms and will facilitate use of credit cards, debit cards, electronic commerce, and other innovative mechanisms to streamline and simplify the process of purchasing appropriate technology. Department procurement vehicles will be established only when necessary for specialized equipment not otherwise available through commercial or other Government vehicles.

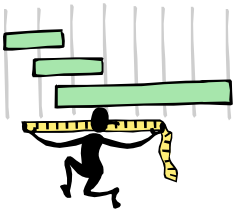
*Improvements in IT require **fundamental changes** in other processes, especially procurement.*

Major Milestones

FY2001

- 25% of unclassified and PC/ LAN/WAN equipment replaced*
- 25% of classified PC/LAN/WAN equipment replaced*
- 10% of post telephone systems upgraded or replaced*
- 20% of emergency radios replaced*
- Updated versions/releases of standard office software installed worldwide*

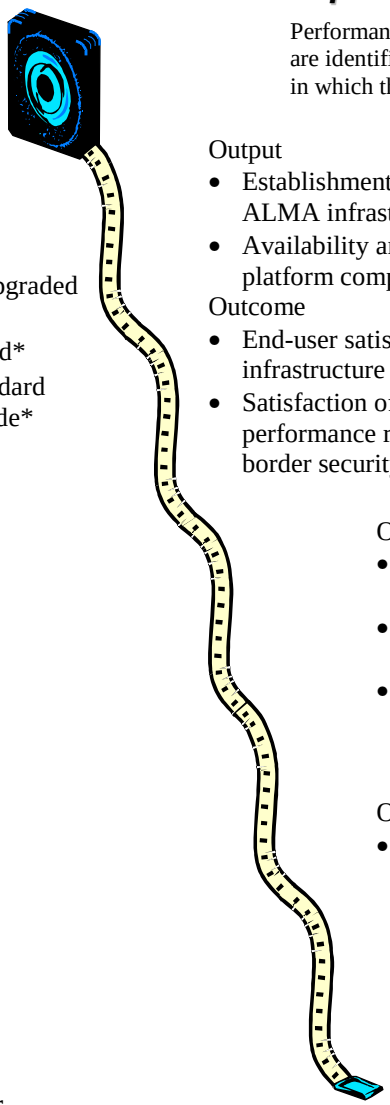
FY2002



* - Milestone is repeated each year.

Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured



Output

- Establishment of a global classified ALMA infrastructure
- Availability and reliability of platform components

Outcome

- End-user satisfaction with classified infrastructure
- Satisfaction of customer performance requirements (e.g., for border security processing)

Output

- Percentage of equipment older than expected (4, 5, or 10 years)
- User perception that equipment and software are up-to-date
- Effective support for mobile computing, including ability to access IT systems, databases, and e-mail from any location

Outcome

- Growth in use of infrastructure equipment and systems, measured by transaction volumes and numbers of database accesses.

External Factors

Other than the availability of funding, there are no external factors that will have a substantial impact on the achievement of this objective.

Objective 1C - Robust Infrastructure Security Services

The Department faces considerable challenges in establishing an effective security infrastructure for the IT environment of the future. Significant shifts in technology and management approach are necessary to meet PDD-63 and safeguard critical IT assets in the modern, highly interconnected era. In the past, the Department has maintained security through a largely closed infrastructure, with few and highly controlled connections to external entities. In this environment, the Department practiced an approach to security characterized as risk avoidance – that is, trying to eliminate all risk. This approach is no longer possible or desirable. As discussed above and addressed eloquently in several other papers[1], our diplomats must be in close communication with their counterparts in other agencies, foreign governments, and NGOs. They must have free and open access to network services, while at the same time, critical IT assets must still be protected.

*Emphasis will shift from risk avoidance to **risk management.***

The purpose of this strategic objective is to establish an evolving security infrastructure that will allow the open communication required for modern diplomacy while protecting the integrity of Department information, networks, and other IT assets. This will require *a shift from risk avoidance to risk management*, under which managers assess the risks and tradeoffs associated with specific situations and determine the level of risk that is acceptable commensurate with the potential threat balanced against the value of openness.

To aid in this ongoing process, the Department will establish under this objective a growing suite of security technologies and services that can be applied to specific situations as appropriate. The technologies and services to be made available will reflect Department-wide requirements for such security features as intrusion detection, digital signature, public key encryption, certificate management, and firewalls. IRM, working with DS, will assess available commercial and government-developed security technologies, and determine which should be made available as standard Department facilities and services. The intent is to consolidate and standardize the provision of security services to the extent possible. The following table lists examples of the types of services to be made available and their uses in applications.

The suite of standard security solutions will be comprehensive. It will secure not only the network, but also systems and applications. Certificates will be used to establish the identity of each user; thereby restricting the type of access to the data based on job requirements or roles. This will enable us to "compartmentalize" databases and allow

*Security technology permits the **secure transport of sensitive information across public networks.***

[1] CSIS, Stimson, and OPAP Reports

different types of users varying levels of access and permissions. We can further secure the data by encrypting the files so that the data is rendered unreadable in the event that the "standard" means of access controls are thwarted.

This objective will result in a fundamental shift in the way the Department develops and integrates systems and applications. Pre-approved security approaches, technologies, and solutions will be provided to Bureau developers to ensure suitable security and consistency. By using standard solutions, the security infrastructure services will enable the Department to exchange information securely with other USG agencies, the public, and nations abroad. This objective will support an effective response to PDD-63 that requires the Department to address the "cyber-threat". The Department's approach is to provide standard enterprise-wide solution sets instead of having everyone invent their own, which could leave gaps to be exploited.

As noted in Objective 1b, the Department will pursue multi-level security (MLS) as soon as the technology becomes available and approved by the National Security Agency (NSA). In the interim, we will establish secure means of exchanging information as required and permitted between the unclassified and classified realms. This will help us keep the total number of desktops down to a minimum. This will require a device to allow exchange of certificate information across the classification boundary to enable seamless, secure exchange of information like secure e-mail supported by Version 3 of Secure/Multipurpose Internet Mail Extension (S/MIME).

The Department has designated the CIO as the senior accountable official for IT security, and has consolidated IT security functions and responsibilities within the office of the CIO. IRM and DS have jointly developed a set of roles and responsibilities that clearly designate the functions of each organization regarding IT security. Within this framework, both organizations will work cooperatively to ensure that the principles of risk management and effective security solutions are implemented throughout the Department.

*Enterprise-wide security depends on the **global directory** included in Objective 1A.*

The two tables, which follow, indicate the primary principles that will be followed and the type and applicability of security controls envisioned.

The benefits to be derived from this objective are:

- Robust security solutions that provide adequate protection while allowing the Department to capitalize on modern communications and information management;

- Standardization of security solutions to increase efficiency, reliability, and to ease the training burden on end-users;

- Standardized security solutions and "reusable" solutions will minimize the review and certification processes; and

- Standard solutions and a universal set of security services will eliminate duplication of effort and foster interoperability among systems.

Security Principles and Concepts

1) *Effective security is an **essential element** of all information systems.*
2) *IT Security should **not unnecessarily impede** business operations.*
3) *Security must be applied **commensurate with the level of risk and magnitude of harm.***
4) ***Security will be applied at all levels** – not just network, but also system, application, and data.*
5) ***The internal threat** exceeds the external threat.*
6) ***Firewalls are the not the only solution** – database encryption will also be used as well as, standard I&A across the enterprise, and modular pre-approved security*
7) *Configurations to eliminate weak links.*
8) ***Security can't be case-by-case**, but must be consistent across the enterprise.*
9) ***Match the applicable solution** to the threat.*

Application of Security Services	*Context/Type of Service Used*
E-Mail	Messages will be encrypted and digitally signed when necessary to ensure confidentiality and integrity.
Virtual Private Network (VPN) to support remote users and locations	VPNs will be established across unsecured or lower security posture, IP networks when feasible to provide adequate capacity and connectivity.
Separate Government-controlled Network	This government-controlled network will handle the most highly classified traffic.
Secure Database Transactions	Bureaus will build systems that rely on a central PKI mechanism to provide secure transactions.
Application Authentication	Transactions will be "signed" to prove authentication before execution.
Information Archiving	Digital Signature techniques will be applied to archived information to ensure integrity.
Secure Web Access	Secure Intranet and Internet access will be established using public key encryption and certificates.
Strong Authentication	Clients/servers will be assured of each other's identity in an electronic transaction using digital signature and certificates.
Document Management	Personal and corporate information will be encrypted. Access to sensitive documents will be controlled via certificates.

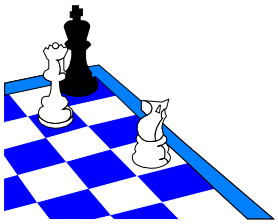
Means and Strategies

The major strategic elements of the Department's approach to IT security are:

- ***Establishing an ongoing infrastructure security program*** – an ongoing program will be put in place to evaluate technologies and approaches. This program will coordinate with internal Department organizations to identify requirements, and will coordinate with other Government agencies (e.g., NSA) and industry regarding best practices. This program will assess commercial approaches, and will seek to exploit the most promising for Department requirements.

- ***Maintaining an IT security architecture segment*** – the IRM Architecture Office is developing an initial security segment architecture to standardize the current set of security solutions to be used. This architecture segment will be maintained over time as technologies and requirements evolve. The security segment will document Department standards and guidance and will explain how to use and apply the standard security solutions.

- ***Coordination*** – historically, Department IT security efforts have been fragmented, and responsibilities have been divided among IRM, DS, and the Bureaus. This has inhibited progress. For the future, the Department will rely on its recent clarification of roles and responsibilities, and will ensure high levels of coordination and consistency. This higher level of coordination will enable the Department to build a series of "pre-approved" and standard security solutions to streamline the security processes.



*The availability of **standard, modular security solutions** will make it easier for users and developers to do the right thing and implement proper security*

- ***Awareness and training*** – the Department will enhance existing security awareness and training programs to ensure that everyone understands the true threats and is able to help spot improper or unauthorized activity. System developers and IT staff will receive separate awareness and training on security solutions so they understand the core services that are available and how to access and use them.

Major Milestones

FY2001

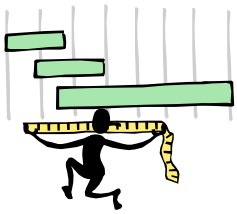
- Open Net protected by firewalls and intrusion detection worldwide
- Comprehensive PKI plan developed for certificate use and management
- Updated security architecture segment published

FY2002

- Plan for standard digital signature capability developed and piloted
- PKI capabilities deployed for certificate management
- Plan for standardized database encryption tools and access controls developed

FY2003

- Pilot test of database encryption tools
- Standard digital signature capability established and made available for use by Bureau and corporate applications
- Updated security architecture segment published

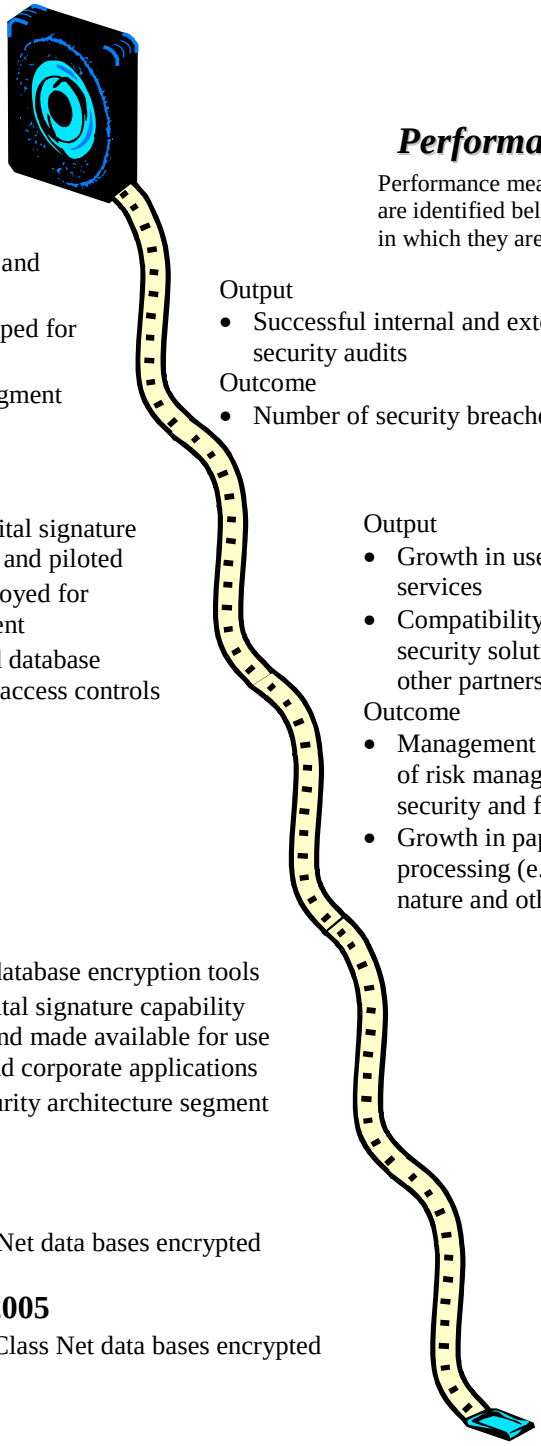


FY2004

- Open Net data bases encrypted

FY2005

- Class Net data bases encrypted



Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured

Output
- Successful internal and external security audits

Outcome
- Number of security breaches

Output
- Growth in use of standard security services
- Compatibility of Department security solutions with NSA and other partners

Outcome
- Management perception of efficacy of risk management in balancing security and functionality
- Growth in paperless transaction processing (e.g., due to digital signature and other security solutions)

External Factors

IT security will be coordinated with key external agencies, including NSA, other members of the international affairs community, and intelligence agencies. Effective IT security is also dependent on advances in commercial security technology, and the Department will monitor developments closely and will establish external partnerships as appropriate.

Objective 1D - Effective Infrastructure Management and Support Services

The Department's IRM Bureau has begun to institute an enterprise-wide IT resource management system (ITRMS) to support the emerging global infrastructure. When fully implemented, the ITRMS will provide integrated remote monitoring and management of all IT hardware, software, and networking components, and will include an integrated help desk capability for end-user support.

The strategic vision for ITRMS is based on the interim solutions currently being developed. This interim capability will provide the following services:

- Real-time monitoring and trouble-shooting of all infrastructure components;
- Configuration management, change control, and tracking of equipment, software, and facilities;
- Integrated help desk to support end users;
- Software distribution and license management;
- Capacity and performance planning and management; and
- Management reporting on IT assets and performance.

The current effort entails both short-term and more strategic initiatives. Under the short-term effort, IRM will integrate existing automated tools and databases to provide an interim capability to support urgent requirements such as Y2K remediation and the integration of State, USIA, and ACDA systems.

Through this strategic objective, IRM will expand on this interim capability and deploy the target ITRMS Department-wide over the next three years. The target ITRMS will be fully integrated and supported by central tools and databases that provide real-time information to all levels of IT support staff and management. The target solution will rely on best practices in use in industry and government. The scope of ITRMS will expand to cover Bureau as well as infrastructure applications, databases, systems, and end-user devices. Help desk integration and consolidation will continue, with many Bureau help desks eliminated and others tightly integrated into the central support infrastructure.

> *ITRMS is key to sustaining the global IT infrastructure while* ***containing the explosive growth in IT costs.***

The Department will also pursue the concept of "seat management" which is gaining prominence in the private sector. Under this concept, either IRM or an outside contractor would contract with Bureaus or the entire Department to provide comprehensive maintenance and support services for a per-seat cost. Required service and performance levels would be specified. The benefits of this approach are predictable costs and service levels.

The benefits to be derived from ITRMS are:

- ***Cost avoidance*** – reducing the rapid growth in need for highly skilled and

expensive staff resources to support the infrastructure.

- ***Infrastructure reliability*** – networks and platforms will perform reliably and IT resources will be available as expected.

- ***Security*** – careful monitoring and support will aid in detection of intruders and any other anomalies that may signal security breaches.

- ***Customer support*** – ready availability of accurate, timely information and automated tools will enable IT support staff to provide the best possible support to end-users.

- ***Infrastructure evolution*** – effective configuration management and monitoring will aid management in making effective and timely decisions regarding replacement and upgrading of equipment, software, services, and facilities.

Means and Strategies

The Department will pursue the following strategies in implementing the strategic ITRMS:

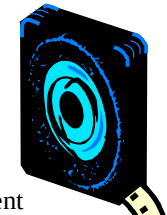
- ***Build on current efforts*** – IRM will use the interim network and system management efforts currently underway to gain experience with enterprise-wide IT management, and will then be well positioned to expand these efforts for the longer-term.

- ***Exploit commercial technologies and approaches*** – the Department has been and will continue to research industry and Government best practices in ITRMS, and will seek out effective partnerships to capitalize on industry success. Outsourcing and seat management will be pursued as appropriate.

- ***Integrate and coordinate*** – to deploy an effective ITRMS in its highly decentralized global environment State will require high levels of coordination among Bureaus and potentially with other foreign affairs agencies. The Department will use the capital investment processes currently being established to foster the necessary levels of coordination. IRM will integrate multiple technologies and approaches in a modular fashion to achieve flexibility and allow for incorporation of technological advances over time.

- ***Common operating environment (COE)*** – the target ITRMS will include a common set of configuration standards for all desktops, servers, and other IT assets – thus constituting a COE. The COE will increase system reliability and manageability, while contributing to favorable TCO.

Major Milestones



FY2001

- Enterprise infrastructure management organization upgraded to target concept
- Common operating environment (COE) documented and pilot tested
- Pilot seat management concept tested

FY2002

- Interim ITRMS assessed and plans for Target solidified
- Target ITRMS deployed at 50% of Department locations
- Consolidated applications management and help desks

FY2003

- Target ITRMS and COE deployed Department-wide

Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured

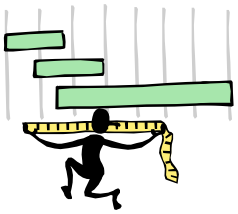
Output
- Growth in use of central ITRMS services
- Extent to which problems are identified through ITRMS rather than in response to user complaints
- Network and system availability and reliability

Outcome
- Average and range of times to respond to users and to correct problems

Output
- Reduction in number of separate help desks
- Reduction in number of network management centers

Outcome
- Average support cost per end user
- Management and end user perception of the quality of support services

Outcome
- Reduction in lost work hours resulting from unavailability of systems



External Factors

Other than the availability of funding, there are no external factors that will have a substantial impact on the achievement of this objective.

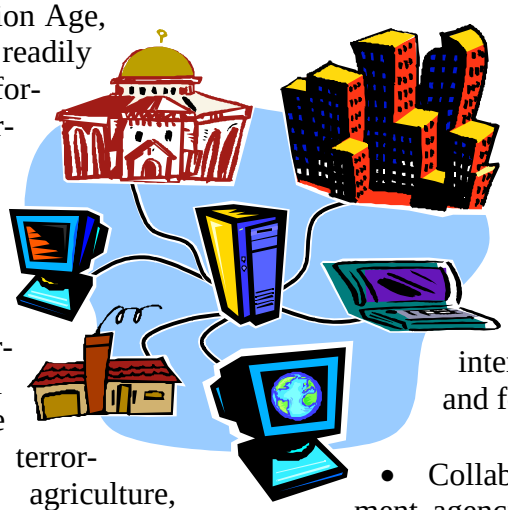
Goal 2 - Ready Access to International Affairs Applications and Information

The conditions under which the Department of State carries out its foreign affairs responsibilities have changed substantially in recent years. People throughout the world now have access to television and the Internet, and through these media follow and help shape public opinion on foreign events as they are happening. The effect of technology has been to make emerging public opinion, at home and abroad, a much more influential factor in diplomacy than it used to be. Also, there are now hundreds of organizations, most of them non-governmental, that are involved in activities impinging on foreign affairs. And, as a by-product of the Information Age, there are thousands of readily accessible sources of information dealing with international matters.

Other US Government agencies are playing an increasing role in international affairs. Issues surrounding international trade and commerce, the environment, international terrorism, law enforcement, agriculture, energy, and others have grown in importance, and the agencies that specialize in these issues have a significant presence overseas. This is in addition to the traditional defense and intelligence agencies operating around the world. The Department of State provides some administrative support to these agencies, and must ensure effective means of electronic communication and connectivity to support the evolving foreign affairs mission.

The shape and perception of international affairs is now heavily influenced by outside organizations; State must monitor the resulting swirl of information that occurs through both official and unofficial channels.

This strategic goal is directed toward applying the Department's technology to the effective conduct of foreign affairs in the Information Age. All employees – but particularly those engaged in substantive, foreign affairs functions – should be able to use the Department's technology to:



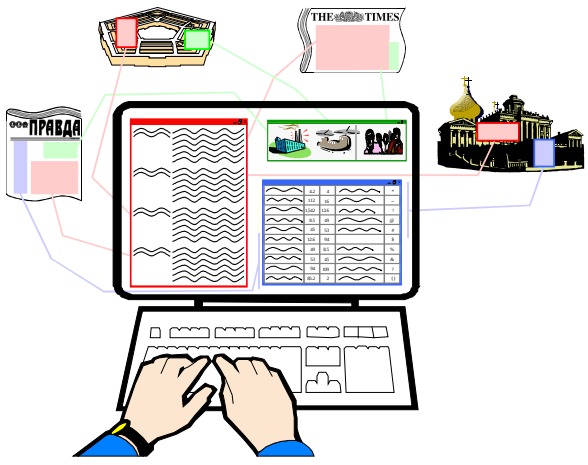
- Gain ready access to international affairs databases maintained by the Department, by commercial and academic organizations, and (where available) by USG agencies, international agencies, and foreign governments;

- Collaborate with government agencies, non-governmental organizations, and businesses involved in routine foreign affairs activities and in the resolution of foreign affairs crises; and

- Provide worldwide audiences with up-to-date information that shapes and informs foreign perceptions of this country's foreign policies and receive feedback from the U.S. public regarding these policies.

Objective 2A - Worldwide Access to International Affairs Information Resources

A wealth of information, such as that found in newspapers, journals, trade magazines, public and non-public information sources, online forums and libraries is becoming increasingly available through online means. The Internet and other modern media have generated extensive resources of previously unavailable information. A considerable subset of this information may bear on the international affairs process. The Department's analysts, whether stationed abroad or in Washington, must have full interactive access to these basic information sources to improve their awareness of events and better support their in-depth analyses. Access to online resources will enhance the ability of analysts everywhere to collect, analyze, and report information and interpret events.



Portal Integrating Narrative, Tabular, and Photographic Data from Disparate Sources

*IT will support **knowledge management** – providing tools for **synthesizing and organizing information** to support foreign affairs analysis.*

This objective is directed toward using the Department's technology to:

- Provide the Department's analysts, desk officers, and policy makers with ready access to all available electronic sources of international affairs, including those commercially available, those managed by the Department, and those maintained by other USG organizations, including the Intelligence Community; and

- Provide the Department's users with facilities that will make exploitation of these databases easy, productive, and useful, even for users faced with short deadlines.

Achievement of this objective will have significant benefits. Foreign Service posts will be able to concentrate their resources on producing more comprehensive analyses and interpretations of events. All Department analysts will gain access to the widest available range of information sources, including new ones that could help broaden their perspectives in interpreting foreign events.

Means and Strategies

In providing employees with electronic access to international affairs databases that range from commercial to intelligence sources, the Department will address two issues:

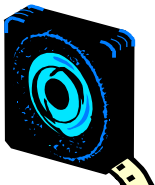
- Security challenges involving the interconnection of Department and outside networks operating at different security levels; and
- Inefficiencies in mining data sources that typically contain much more chaff than wheat.

The Department will address security issues through its risk management strategy, and will allow wider user access to databases within the constraints of national security classification rules. Thus, Open Net users will have full access to Unclassified/SBU databases and Class Net users will have full access to databases up through the Secret level. Sufficient security facilities will be provided to allow users to access through their Class Net workstations a variety of databases maintained on unclassified and lower security-level networks.

In order to make user access to the international affairs database both productive and easy, the Department plans to:

- Accumulate useful State and non-State information in internal Department repositories that ensure rapid access and high levels of relevancy of materials retrieved. These data repositories, located on super-servers in the Department's headquarters computer facility, will support Department users on a worldwide basis.
- Implement a standard web portal interface, a standard search engine, and a single method for formulating queries against data maintained in this repository;
- Establish a knowledge management process through which sophisticated tools will be applied to leverage the entire breadth of information available to State employees. Tools for data organizing, data mining, search and retrieval, profiling, and both "push" and "pull" access to information will be used in this pursuit.
- Tailor the contents of the repository databases to meet the general requirements of Department users, rather than the specialized requirements of source organizations providing the databases. For example, the repository's version of the Central Foreign Policy File will include substantive documents for the most recent five years, instead of all documents for a 25-year period – a reduction of approximately 90% that will improve search speeds and minimize irrelevant materials retrieved; and
- Provide effective directories to important databases that cannot be included in the repository.

In tailoring databases to achieve easy and productive use, the Department plans to employ subject matter specialists to prescreen the materials – i.e. to decide which documents and databases are to be included in the Department's international affairs repository.



Major Milestones

FY2001

- International affairs repository established
- International affairs database management organization created

FY2002

- Directory of Internet data sources created
- Useful Internet international affairs information included in repository

FY2003

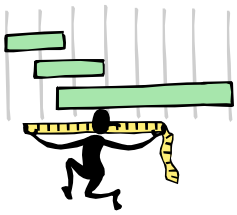
- Central Foreign Policy File, other Department databases included in repository
- All domestic users provided access to repository

FY2004

- All overseas users provided access to unclassified repository

FY2005

- All overseas users provided access to classified repository



Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured

Output

- Number of daily accesses to repository

Output

- % of Department employees with online access to repository

Outcome

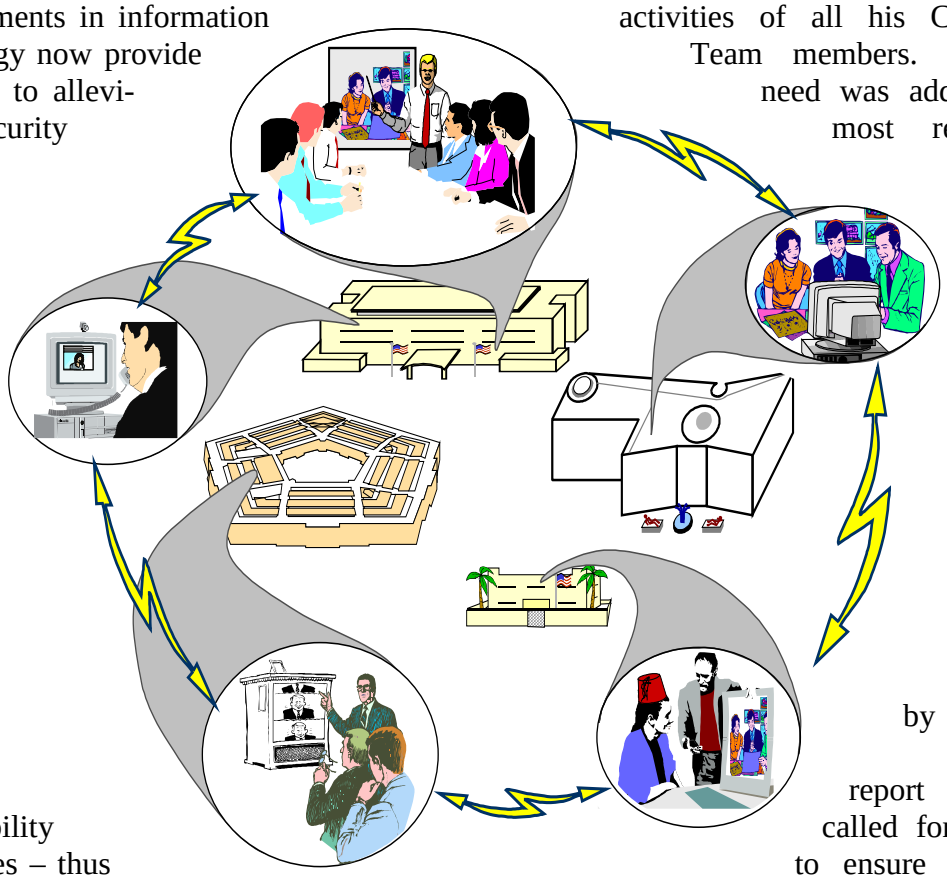
- User evaluations of repository usefulness in:
  - keeping abreast of international affairs
  - generating policy documents
  - initiating useful contacts with others involved in international affairs

External Factors

Other than the availability of funding, there are no external factors that will have a substantial impact on the achievement of this objective.

Objective 2B - IT Support For Effective Collaboration

Effective collaboration within the foreign affairs team and between members of the foreign affairs community has always been a critical challenge to the Department. In addition, the growing numbers of organizations now at the periphery of foreign affairs activities make it increasingly difficult for the Department to monitor the work of and collaborate with all of the relevant parties. Given the worldwide nature of the collaboration, electronic interaction is the only practical way to do so. Recent improvements in information technology now provide the tools to alleviate security and compatibility challenges – thus facilitating the strengthening of the Department's leadership role in U.S. foreign affairs.



Enhanced collaboration leverages technology to: 1) strengthen the effectiveness of **traditional** diplomatic teams; and 2) build and operate **virtual** diplomatic teams, whenever the situation warrants.

One traditional diplomatic team that technology can help strengthen is the Ambassador and his Country Team members. Especially with the steady proliferation of non-Department organizations at post, it is essential that the Ambassador, as the President's representative, be able to communicate electronically with and supervise the activities of all his Country Team members. This need was addressed most recently and clearly by the OPAP report which called for State to ensure an IT infrastructure that supports connectivity among agencies operating at post. A second traditional diplomatic team that technology can help strengthen is the Department's crisis management operations. Task Force members in the Operations Center

and the Bureaus of Consular Affairs and Diplomatic Security must have the best technology available to interact not only with each other, but with their counterpart USG organizations and with any other organizations that may have a role in a particular foreign situation. Traditional diplomatic teams, such as these, will be strengthened by giving them secure electronic interconnections with their colleagues.

*Effective collaboration requires **secure multi-point interconnections.***

Technology now makes possible the effective operation of virtual diplomatic teams – that is, groups composed of geographically separated members who may interact on a real-time basis to address urgent problems. Communications and software that support multi-point videoconferencing, online discussion groups, and joint production of documents now make it possible for virtual teams to operate together almost as if they were physically co-located.

Over a period of time the Department expects virtual diplomatic teaming to assume many forms not fully anticipated today. For example, cables that are now sent from the field to Washington will probably be replaced by documents created jointly by one or more post officers, Washington-based desk officers, intelligence officers, members of other USG agencies, and, in some cases, representatives of NGOs and foreign governments. Since such documents will have their origin at multiple locations, they will reflect the different perspectives of the locations and organizations involved, and they will no longer need to be "sent" in the traditional sense but, rather, posted to a repository and made available for review by interested parties.

Virtual teaming may well be the dominant way the Department conducts its business in the future. It is easy to visualize electronic interactions among the entire international affairs community covering the whole range of foreign affairs activities, including:

- The Department's counter-terrorism officers in an online forum with the FBI, post and regional security officers, and with local law enforcement officials in the appropriate countries;
- Arms control experts from several USG agencies and foreign countries reviewing bills of lading for possibly illicit arms shipments;
- Human rights officers consulting with local sources to verify and document reports of abuse;
- An Embassy commercial officer in a videoconference with officials of several U.S. firms and Federal agencies (e.g., Commerce, Trade, Small Business Administration) to discuss a recently-discovered trade opportunity; and
- Environmental officers from State and EPA consulting with scientists and other affected individuals and organizations from a number of countries in the process of developing international agreements.

As technology permits, these types of interactions among those involved in foreign affairs activities will become ever more commonplace.

*The job of IT is to provide a **backbone for e-diplomacy**.*

Achievement of this objective will have significant benefits. It will give the Department a continuing ability to exert a leadership role in U.S. foreign affairs. It will provide Ambassadors with an increased ability to manage country teams. It will give the Department's Operations Center an improved ability to manage diplomatic crises. And it will enable all Department employees to work closely not only with their own colleagues, but also with members of other organizations, on the development and execution of foreign policy.

Means and Strategies

To improve its effectiveness in collaborative diplomacy by means of technology, the Department needs, first of all, to give priority focus to that aspect of its work and then find ways around the technological and security impediments that stand in the way of such electronic collaboration. This strategic objective provides the focus for that effort and will lead to the appropriate resources needed to achieve it.

The Department plans to implement collaborative diplomacy through a number of separate, but related, initiatives. The first of these will focus on ambassadorial management of country teams. The Department will ensure that the Ambassador in each country can communicate electronically with each Country Team member at post, no matter what differences in security levels may exist. In addition, the Department will implement a standard Ambassador Country Team software package, built to the specifications of Ambassadors and reflecting their needs at missions of different sizes and characteristics.

The IRM Bureau will work with its counterparts in other agencies operating overseas to establish interagency connectivity. Work is already underway to plan pilots to explore technological solutions for supporting robust connectivity among multiple overseas agencies. Interagency working groups will be established to further this objective.

The Department also plans to strengthen the technology supporting the Operations Center Task Force areas and other crisis management centers in the Department. Effective linkages among these various centers and specialized IT tools will be provided to foster:

- Close collaboration in crisis management among multiple locations in essentially the same way as if crisis managers were co-located;

- Intelligent access (e.g., using pattern recognition and data mining) to cur-

rent and historical information on similar or related events;

- Efficient and effective case management; and

- Substantive decision support.

These IT enhancements will improve collaboration with other Operations Centers – e.g. Defense, Central Intelligence Agency, Federal Aviation Administration, Justice, and the Federal Bureau of Investigation – as well as U.S. Embassies abroad.

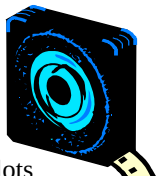
The Department also plans to reinforce the efforts already made by Functional Bureaus – notably the Bureaus of Economic and Business Affairs, Public Diplomacy, Oceanic, Environment, and Scientific Affairs, and Democracy, Human Rights and Labor Affairs, to achieve collaboration with a range of USG and non-governmental organizations working on global issues of the economy, environment and human rights.

As part of this overall effort, the Department will establish a test environment to determine the potential future effectiveness of virtual diplomatic teaming, both in the conduct of routine Departmental business and in the management of crises.

Major Milestones

Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured



FY2001

- ⌂ Country team management system implemented
- ⌂ Interagency connectivity/access pilots initiated, following OPAP recommendations

FY2002

- ⌂ Internal Department crisis centers fully linked

Output
- Percent of Ambassadors with full country team system capabilities

FY2003

- ⌂ Inter-agency collaborative system implemented
- ⌂ Inter-agency crisis centers linked

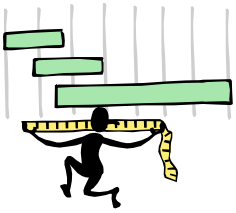
Outcome
- Evaluations of Ambassadors regarding contribution of system to country team management

FY2004

- ⌂ NGO collaborative system implemented

Output
- Number of other-agency crisis centers linked to Department's crisis centers

Outcome
- Evaluation of Operations Center regarding effectiveness of electronic tools for crisis management



FY2005

- ⌂ Crisis center network and Foreign Service posts linked
- ⌂ Foreign government collaborative system implemented

Output
- Number of posts linked to crisis center network
- Number of foreign governments linked to Department's collaborative network

External Factors

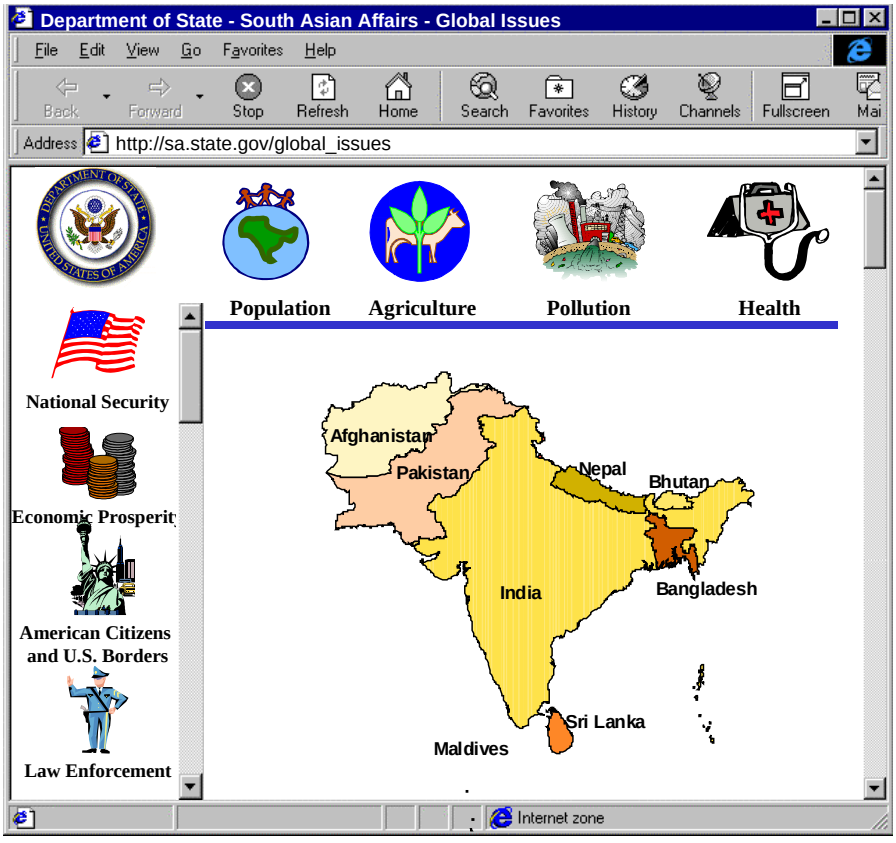
Other than the availability of funding, there are no external factors that will have a substantial impact on the achievement of this objective.

Objective 2C - Effective IT for Public Diplomacy

In October the United States Information Agency (USIA) and the Department's Bureau of Public Affairs were consolidated to create a new Bureau of Public Diplomacy. Enhanced technology will improve the ability of this new combined entity to keep U.S. and foreign publics apprised of foreign affairs issues and activities. In a February, 2 1999 letter to USIA employees, the Secretary of State wrote: *"Let me close by saying that as far as Public Diplomacy is concerned, my motto is not "less is more," but rather "more is better." The world is changing, and the full integration of public diplomacy into American foreign policy will make it more agile and open, and more convincing to the rest of the world."*

For a number of years PA, in conjunction with the University of Illinois, has operated the Department's Web Site. This Web Site offers much up- to-date information, including recent statements of the Secretary of State and other officials regarding foreign policy matters. A recent independent evaluation ranked it among the most highly rated Web Sites maintained by government or private organizations. Also, the Bureau of Consular Affairs has maintained for some time highly effective citizens' services information systems utilizing web technology.

In addition, in past years, overseas elements of USIA developed Web Sites for approximately 40 U.S. Embassies abroad. These Web Sites are directed toward foreign populations (the Smith-Mundt Act forbids USIA to target the U.S. public in its publications), although they are available to anyone with access to the Internet.



This objective has two major elements:

1) Making readily available to the U.S. and foreign publics in an easily understandable form the key elements of U.S. foreign policy, including its objectives, approaches, and results achieved; and

2) Providing a mechanism for the U.S. public to register their opinions and suggestions regarding U.S. foreign policy.

Achievement of this objective will have significant benefits. The U.S. and foreign publics will have up-to-date, succinct descriptions of U.S. foreign policy and international issues. The U.S. public will also have the ability to interact with foreign affairs leadership principals and to express opinions regarding foreign affairs matters. The Department will have an effective way to communicate with the public and receive input from them regarding their views of foreign policy matters.

*The Department must interact electronically with today's **"wired society"** to implement effective public diplomacy.*

Means and Strategies

The Department's existing Web Site will be the foundation for improving the Department's efforts in public diplomacy. With the addition of USIA, the new Public Diplomacy Bureau is admirably equipped to manage the Web Site, either by itself or in a continuing partnership with the University of Illinois.

The Department plans to maintain on its Web Site up-to-date statements of U.S. foreign policy covering both bilateral and global issues. This will make it easy for the public to determine, for example, what U.S. bilateral and multilateral policies are and, also, what their historical bases are.

The Department plans to implement various mechanisms for interacting with the U.S. public. These may include: a weekly report and/or online discussion involving the Secretary, the Deputy Secretary, and the Under Secretaries for Political, Economic, and Political Military Affairs; periodic discussions on bilateral matters led by U.S. Ambassadors; Department-sponsored symposia between foreign affairs scholars and the public; and a mechanism for the public to air their views on foreign policy matters and receive an electronic acknowledgement from the Department.

Major Milestones

FY2001

- Comprehensive foreign affairs policy statements promptly available

FY2002

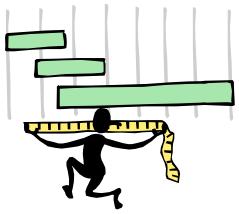
FY2003

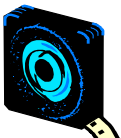
- Two-way interactive discussion capability with US public implemented

FY2004

FY2005

- Regular foreign affairs Internet town hall meetings established





Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured

Output

- Number of policy issues adequately covered
- Number of accesses to web site

Output

- Average age, in days, of documents when posted

Outcome

- Public evaluations of the utility of the Web site

Outcome

- Department evaluations of the utility of public comments

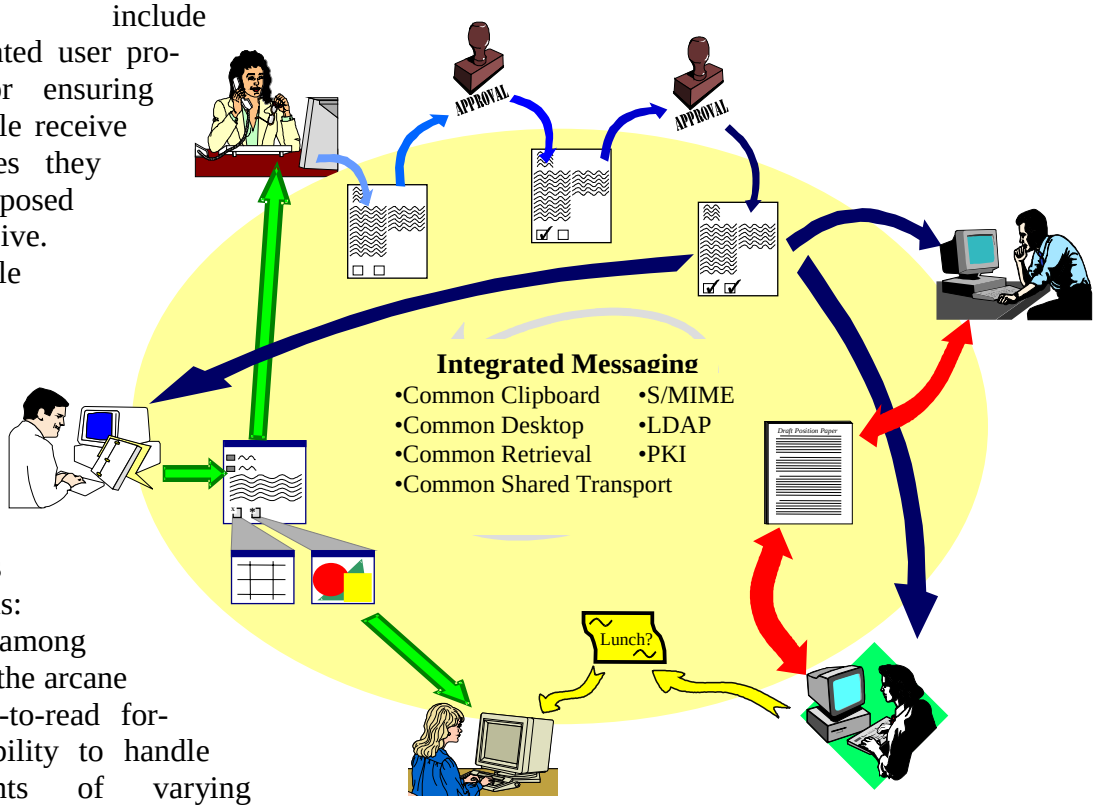
External Factors

The Smith-Mundt Act may impact the Department when implementing the types of web sites described in this objective.

Goal 3 - Integrated Messaging – A Modern Worldwide Approach

The Department is highly dependent on "messaging" systems for a range of functions and processes. Traditional cables or formal record message traffic are used for communicating official Department policy; transmitting administrative transactions, and issuing command and control directives. Cable traffic includes classified information, and both individual and organizational messages. Cables are processed and routed through an outmoded network of switches and application programs, which include sophisticated user profiling for ensuring that people receive the cables they are supposed to receive. The cable system has numerous limitations: notable among them are the arcane and hard-to-read format, inability to handle attachments of varying types, and difficulty integrating cable-based information into other standard applications and processes. At the same time, the cable system embodies several characteristics that are vital to the Department's mission and must be retained:

- Authority – people recognize cables as official communications that "speak" for an organization or the entire Department
- Organizational messaging – cables can be directed to organizations as well as individuals
- Security – cables support transmission of classified national security information, and distribution is based on profiles and built-in need-to-know rules



- Archiving and record retention – the cable system is closely linked with the Department's archiving system, meeting Federal requirements for records management

The Department has become increasingly dependent on electronic mail over the past few years, and efforts are well underway to standardize on a single e-mail package Department-wide. E-mail is now the mechanism of choice for all types of informal messaging, including transmission of reports of important substantive and administrative information, as well as more personal messages. E-mail usage is increasing rapidly at the same time that cable traffic is decreasing. This trend is likely to continue as electronic mail offers greater flexibility and ease of use than cables, and e-mail information can be readily integrated into word processing documents and other applications. The limitations of e-mail are the lack of some of the formal structures contained in the cable system – e.g., user profiling, automatic routing and approval processes, and security features. In short, e-mail lacks the authority of formal cable traffic.

New best-case business processes and technological solutions will be used to provide the requisite Cable features.

During the planning horizon of this strategic plan, the integration of formal and informal messaging will increase. The ongoing implementation of CableXpress is a step in the process of blurring the distinction between the two. Through CableXpress, cables are delivered to a user's desktop in a form much like e-mail. Cables thus delivered can be pasted into word-processing documents on the user's desktop. In the future, formal messages will support attachments of all types, and will incorporate all features of business quality electronic mail. At the same time, they will retain the authority and formality of official record traffic.

Key characteristics of today's cable will not be lost in the modern integrated messaging approach

Through this goal, the Department will assess and thoroughly re-engineer the way it performs all types of messaging. It will examine all current uses of cables and e-mail, and determine the best business processes and technological solutions for each use. Clearly, the cable system is used today for some functions for which it is ill suited – e.g., routing administrative transactions such as travel orders and personnel transactions – since, in the past, there was no good alternative. In the future, the Department will establish a single enterprise-wide business-quality electronic mail system for those uses of messaging best served by e-mail. Other uses of the cable process will be supported by innovative technologies suitable for transaction processing – e.g., message

Key elements required for messaging success:

- ***Robust network with scalable capacity***
- ***Global directory with unified identification and security information***
- ***Modern message transport and delivery approaches – push and pull, intelligent searches, user-defined interfaces***
- ***Consolidation of storage and retrieval facilities to reduce fragmentation and ensure supportability***

brokering utilities, web-based transaction processors, groupware, workflow, and database-based applications. Still other uses, e.g., specific administrative transactions, such as procurement, will be replaced by function-specific off-the-shelf applications as currently being pursued by Logistics Management, Personnel, and other Bureaus.

The Department will take an approach that integrates all messaging requirements through a variety of Commercial Off-the-Shelf (COTS) techniques

For a long-term solution, the Department will draw on a variety of messaging options including, for example, the new Defense Messaging System, and evolving commercial offerings. A single solution is unlikely to address all requirements, and so a COTS integration approach will be pursued. The following general requirements and priorities will be supported:

- Preserving requisite features of the cable system;
- Providing secure interoperability between the Department and newer classified message systems (e.g., the Secure Internet Protocol Router Network (SIPRNET), or information and process sharing with other USG organizations, NGOs, and the public;
- Enabling operational streamlining by means of applications that can "message" information to one other as transactions are processed; and
- Unifying the media and the message, incorporating new message formats and media such as attachments, tables and spreadsheets, graphics and photographs, biometrics, video and voice.

The re-engineering of the messaging processes of the Department will yield the following key benefits:

- Robust electronic mail that is easy to use and allows rapid and reliable transmission of business and mission critical information, both classified and unclassified;
- Ability to attach and integrate any form of information into electronic mail messages;
- Support for special Department requirements, such as profiling and search terms, to aid in retrieval;
- Integration with official State archiving system, including efficient and effective search and retrieval functions;
- Innovative capabilities to enhance and streamline transaction processing;
- Innovative technologies to aid in collaborative processing among teams and work groups, no matter where they are located; and
- Ability to access all of these messaging capabilities from anywhere in the world, including non-State locations, through laptop computers, telephones, and other end-user devices as the technology evolves.

Modernized messaging is a prerequisite for attainment of other strategic IT and Department goals. Operational streamlining (Goal 4) requires new messaging technologies noted above – e.g., message brokering to streamline the flow of information among disparate

applications. The infrastructure described in Goal 2 will be based in large part on a robust replacement for today's cable system, along with enhancements that permit attachments, secure internal and external communication, and collaborative processing. The integrated messaging system contemplated under Goal 3 will provide much of the needed infrastructure.

These benefits will be achieved through pursuit of the two strategic objectives described in this chapter.

Objective 3A - Business Quality Electronic Mail

The Department will establish a single state-of-the-art worldwide electronic mail system that supports all requirements of the current formal and informal systems for transmission of messages. The e-mail solution will replace the existing fragmented suite of electronic mail and cable systems with a single, centrally managed system. The system will be standards-based, and will thus support internal and external communication, including handling of attachments of all sorts. The system will also include a standards-based enterprise-wide directory that can be used by other applications as well.

The e-mail system of the future will include sophisticated expert systems features to ensure proper routing of message traffic. Organizational messaging will be accommodated, as well as person-to-person e-mail. Security and data integrity will be emphasized to ensure that no messages are lost or misdelivered. Digital signature will support authentication and non-repudiation when needed. Classified traffic will be accommodated, and guard technology will enable authorized users to move unclassified portions of messages from the classified to unclassified environment for further processing.

Best practices and industry benchmarks will be used to design and deploy a robust e-mail solution.

The e-mail system will rely on the infrastructure and standard services to be installed under Goal 1. The security services to be developed under Strategic Objective 1C will address the security requirements noted above. The design and development of e-mail will be closely coordinated with the modern global network, global directory, and other infrastructure development initiatives under Objective 1A.

Means and Strategies

The key strategy for achieving this objective is to conduct a thorough business process re-engineering (BPR) effort to explore all Department requirements for business quality e-mail. The BPR will examine all current uses of cables and e-mail and determine which should be supported by the new e-mail system. The BPR will determine requirements for security, profiling, search and retrieval, and archiving.

Once the requirements are thoroughly defined and reviewed broadly in the Department, the BPR will continue to identify the best available commercial e-mail technology to support the Department. The chosen solution will be standards-based and sufficiently robust to support the Department worldwide.

Major Milestones

FY2001

- BPR completed and requirements analysis phase completed

FY2002

- Messaging approach designed and pilot-tested using modern infrastructure (global directory, security services)

FY2003

- Implementation plan developed and deployment begun
- Deployment 25% completed
- Expert system for record retention and archiving for messages

FY2004

- Deployment completed and cable processing terminated
- Secure messaging (person to person) with external organizations established

Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured

Output

- System availability, reliability, performance

Outcome

- Required characteristics of formal messaging retained
- Growth in usage of the new system

Outcome

- Elimination of cable process
- Accuracy of record retention process

External Factors

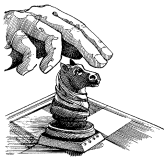
Other than the availability of funding, there are no external factors that will have a substantial impact on the achievement of this objective.

Objective 3B - Standard Utilities and Services for Information Exchange

The focus of this objective is to create an innovative suite of services and utilities that can be shared throughout the Department to move information efficiently and reliably, with minimal custom development. The Department will capitalize on industry best practices and deploy such technologies as message brokers, transaction brokers, workflow engines, correspondence and document management systems, imaging technologies, and web-based technologies for handling diverse transactions in standard ways. The basic web browser is an example of such a technology – it can be used to browse and search for information, and can also be used to execute secure purchase transactions.

The customers for this objective are the systems managers, designers, and developers throughout the Department. This objective will be successful if these customers use the chosen technologies, thus enhancing the functional systems they can offer to end-users. This objective will result in increased standardization of processing throughout the Department, thus reducing the support and training burden. This objective will also reduce the time and risk for major systems development efforts.

New best-case business processes and technological solutions will be melded to streamline transaction processing via messaging approaches.



Means and Strategies

Under this objective, the Department will explore best practices in industry and government to identify the most promising approaches and technologies for information exchange. Candidate technologies will be pilot-tested in domestic and overseas environments, and those that prove successful and effective will be implemented and made available for Department-wide use.

Specific strategies that will guide the pursuit of this objective are:

- ***COTS integration*** – off-the-shelf products will form the backbone of the messaging environment. These products will not be customized, but will be integrated.

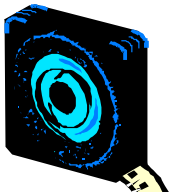
- ***Personal and organizational archiving*** – standard utilities will be provided to enable end-users and organizations at any level to establish, access, share, and easily maintain archives of key message data.

- ***Technology evolution and flexibility*** – the Department will avoid locking itself into dead-end approaches and solutions; instead, it will use standards-based products and technologies that evolve with the private sector.

- ***Process streamlining*** – this objective will support and be coordinated with Goal 4, which focuses on radical streamlining of the Department's operations. Objective 3B will provide a key part of the infrastructure – standard processes for transaction routing – needed for streamlining operations. This objective will also draw on Goal 4 work done in data administration.

Major Milestones

Performance Measures



FY2001

- BPR completed and requirements analysis phase completed

FY2002

- Initial pilot tests planned and conducted

Output

- Pilots successful and completed on time
- Successful identification of promising message-based technologies and approaches

Outcome

- Extent to which new technologies are used

FY2003

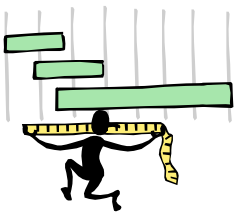
- Personal and organizational archiving established and linked to record archiving
- Implementation plans developed and products made available for Department use

FY2004

Products deployed domestically

Outcome

- Cost savings for software and interface integration/ development



FY2005

- Standardized message-based infrastructure for inter-system transaction processing and interface management

External Factors

The success of this objective is dependent on advances in technology for automated record retention in accordance with Government requirements. In addition, the Department must adhere to prevailing standards, as many functions supported by this objective will entail automated interaction with external organizations, for example, the Office of Personnel Management (OPM) for personnel transactions, and the General Services Administration (GSA) for procurements.

Goal 4 - Leveraging IT to Streamline Operations

Advances in information technology create a tremendous opportunity for the Department to enhance and streamline administrative and substantive operations, increasing productivity and effectiveness. Government and commercial organizations are capitalizing on IT to speed up processing of virtually all types of transactions. Through standardized, easy-to-use systems, end-users can quickly accomplish transactions that in the past had taken days or weeks and involved the efforts of many people. The types of advances typified by the Internet and the Government purchase card – where people can rapidly purchase goods and services – reflect the wave of the future.

> In the future, people will be able to conduct virtually all business **electronically and autonomously**.

Two key prerequisites must exist to enable the Department to streamline effectively. First, the global infrastructure specified in Goal 1 must be established. Reliable, secure, scalable, and high capacity networks and platforms are a must. Second, the Department must consolidate and standardize IT processing resources – servers, databases, and applications. This second prerequisite is a key component of this Goal 4.

> *We must **consolidate and standardize** to realize the benefits of IT.*

The Department's highly distributed computer topology was established during an era in which inadequate communications made it necessary to distribute equipment and data to user sites. This distributed IT environment has created major problems for the Department and is no longer appropriate. Among the problems are: the burden of operating and maintaining many more computer facilities than necessary; a multiplicity of locally-developed, non-standard software systems; fragmented administrative information; and technical difficulties arising from the need for many separated computers to exchange data.

The world's increasing reliance on the Internet, both for professional and personal purposes, is transforming IT and the way people conduct business. From their homes, Department employees are now able to perform a wide variety of on-line functions, including banking, procuring needed goods, updating and searching databases, and other such functions that are characteristic of the Department's administrative operations.

The transformation of traditional processes from paper-based to electronic workflow has already facilitated the streamlining of some operations, as evidenced by the well-established and highly successful consular and personnel processing operations. The Department's shift toward modern commercial communications will enable the Department to extend this streamlining to the worldwide point of origin, thus empowering the end-user both to initiate and complete transactions.

Nevertheless, for a variety of reasons, Department users do not yet have full authority to effect transactions in the internal administrative systems, despite the potential efficiencies inherent in this

approach. It is time to give Department employees the ability to use the Department's internal administrative systems in much the same way they are able to use commercial systems.

This focus of this goal is twofold:

- Empower the users of administrative and consular systems by providing them with the online ability to complete virtually all transactions for the Department's financial, procurement, personnel, property, travel, selected consular functions, and other systems; and

- Take advantage of improved communications to consolidate computer/communications and support facilities, thereby reducing the excessive personnel and dollar costs required to maintain a world of distributed computers.

Objective 4A - User-Empowered Administrative Systems

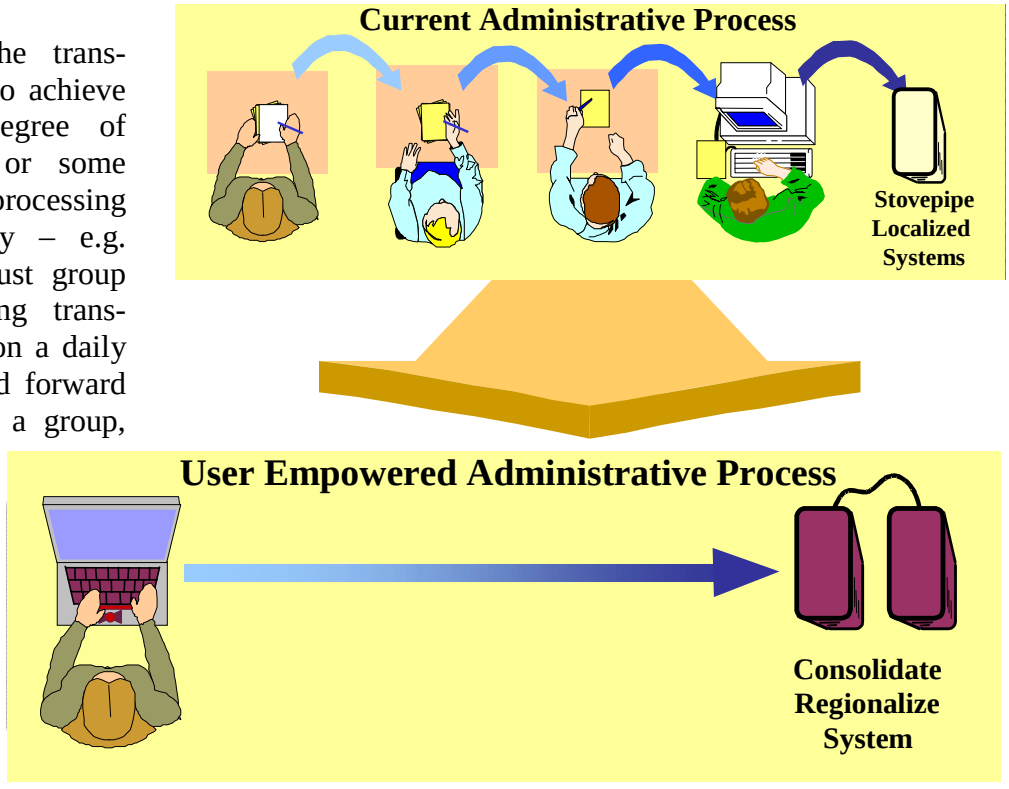
The presumption underlying many of the Department's administrative systems is that individual users cannot be allowed to complete transactions on their own. Intermediaries between the users and the "official" administrative databases must exist to perform one or more of the following functions:

- Authorize and control transactions – e.g. users can originate requisitions, but cannot generate associated purchase orders and obligations: these must be done by procurement and funds specialists;

- Protect the database - e.g. employees cannot directly update their personnel audit records, but must submit forms to be keyed by personnel specialists; and

- Batch the transactions to achieve some degree of control or some type of processing efficiency – e.g. posts must group accounting transactions on a daily basis and forward them as a group, rather than updating the official files, as a by-product of each individual transaction.

Separation of functions helps to guard against fraud, but the costs associated with fragmented and duplicate processing are high. The multiple handling of transactions is wasteful and slow – so slow, in fact, that most posts and domestic offices have built their own systems to track the status of transactions as they progress through various processing layers. The Department devotes untold staff hours to the double and triple handling of relatively low-value transactions and then to the double and triple checking of where those transactions stand at any given moment.



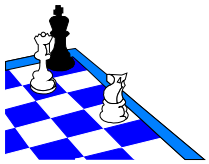
The technical means now exist for the Department to empower users to effect most administrative transactions themselves and to do so during a single sitting at their workstations. Authorized users should be able to effect most procurement actions completely and quickly. Even if a funds check is required, this should take no longer than the few seconds that credit card companies require to check the status of commercial purchasers. And since most items the Department needs to acquire can be purchased over the Internet, the bulk of procurement actions can be greatly streamlined.

User empowerment requires ***standard, easy-to-use systems, with uniform interfaces*** *– like the web.*

Users should also be empowered to update and search financial, personnel, and property records online. There should be little need for administrative specialists in the various areas to be involved in the transactions while they are occurring. Rather, specialist support groups should be able to devote their resources to: providing help to users; carrying out high-value transactions beyond the authority levels of individual users; and conducting after-the-fact audits of transactions to ensure that users are carrying out their responsibilities properly.

Empowering the users of administrative systems will have significant benefits. It will improve user control over their own transactions and operations. It will improve the quality of data in the administrative systems by pinpointing responsibility for that data. And by eliminating the multiple processing of transactions it will substantially increase the productivity of employees conducting administrative operations.

Means and Strategies



One of the Department's key strategies for empowering its administrative systems users will be to make its internal systems emulate the commercial systems - e.g. online personal banking and financial services - with which those users are familiar. This emulation will include not only procedural aspects of those systems, but also the web-based look and feel of the user interface.

As administrative transactions occur throughout the world, they will be posted in an authoritative repository that will be available for online retrieval and analysis. Such co-location of data will be a proxy for the full integration of administrative systems that, given the dependence of various sub-organizations on different COTS software packages, the Department seems unlikely to achieve.

The Department plans to exploit electronic commerce as one of the main mechanisms driving its movement toward user-empowered administrative systems. The ready availability of multiple sources through the Internet, including government-wide procurement vehicles, will satisfy USG competition requirements, as long as users follow prescribed procedures. Specialized and

high-value procurements will continue to be carried out by procurement specialists, but this is a small percentage of the Department's volume of acquisitions. Speed of delivery of items acquired through electronic commerce will, in many cases, obviate the need for warehousing and warehousing systems.

The financial implications of electronic commerce are profound. Pre-authorized credit card funds will continue to be used for low-value items, but online authorizations of larger obligations based on funds status will be made available to remote users within a matter of seconds, as is done in the commercial world.

The Department's system for reporting on purchases will also emulate the commercial sector. Monthly, quarterly, and annual summaries of completed transactions, indexed by computer-applied object class and function codes, will provide the basis for individual accounting reports. The central administrative repository will be available for additional detailed reports and analysis, if needed.

***Database integration** is essential to enable user - empowered transaction processing.*

For maintenance of its personnel and property records, the Department will provide users with the facilities to update official records directly and, at the same time, place full responsibility on them for doing so. This approach will result in higher quality data than now exists, will reduce the number of middlemen now involved in these operations, and will make possible the concentration of worldwide information at a single location, thereby providing the Department's resource managers with a concentrated source of administrative information.

***Smart cards** will consolidate information and functionality – security, personnel, travel, budget, etc.*

Changes of the type outlined above require serious investigation and planning before they can be carried out. Several administrative organizations are currently engaged in BPR studies and/or the implementation of new procedures arising from such studies. Thus far, however, the focus has been more on the needs of the administrative organization conducting the study than on a user-centric view of how to harness technology to make administrative systems look and operate like commercial systems.

Consular systems will also employ advanced IT to empower consular officers and enhance border security, building on the successful, modernized Consular Affairs systems in place today. Among the technologies that may be used to streamline and improve border security and other consular operations are: biometrics, remote video interviews for passport and visa adjudication, electronic travel documents, and kiosks for entry and retrieval of information.

***Standard solutions** will largely replace post and Bureau-specific systems.*

The Department plans to continue and extend the BPR studies of its administrative operations, and focus on emulating the paradigm shift that is already well underway in the commercial sector.

Enterprise Resource Planning (ERP) systems will be explored as a means to achieve post and enterprise-wide integration.

Major Milestones

FY2001

- BPR studies of administrative systems completed
- Revised administrative procedures published

FY2002

- Personnel, property, financial, procurement systems re-faced

FY2003

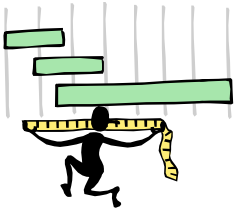
- User-empowered systems for domestic operations
- Consolidated administrative data repository established

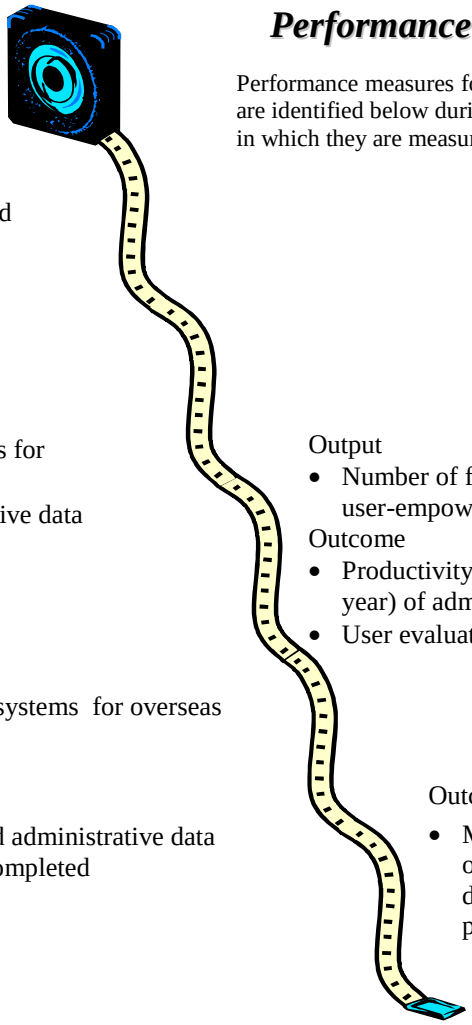
FY2004

- User-empowered systems for overseas operations

FY2005

- Consolidated administrative data repository completed





Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured

Output

- Number of functions supported by user-empowered systems

Outcome

- Productivity (transactions per staff year) of administrative users
- User evaluations of systems

Outcome

- Management evaluations of utility of consolidated data for management purposes

External Factors

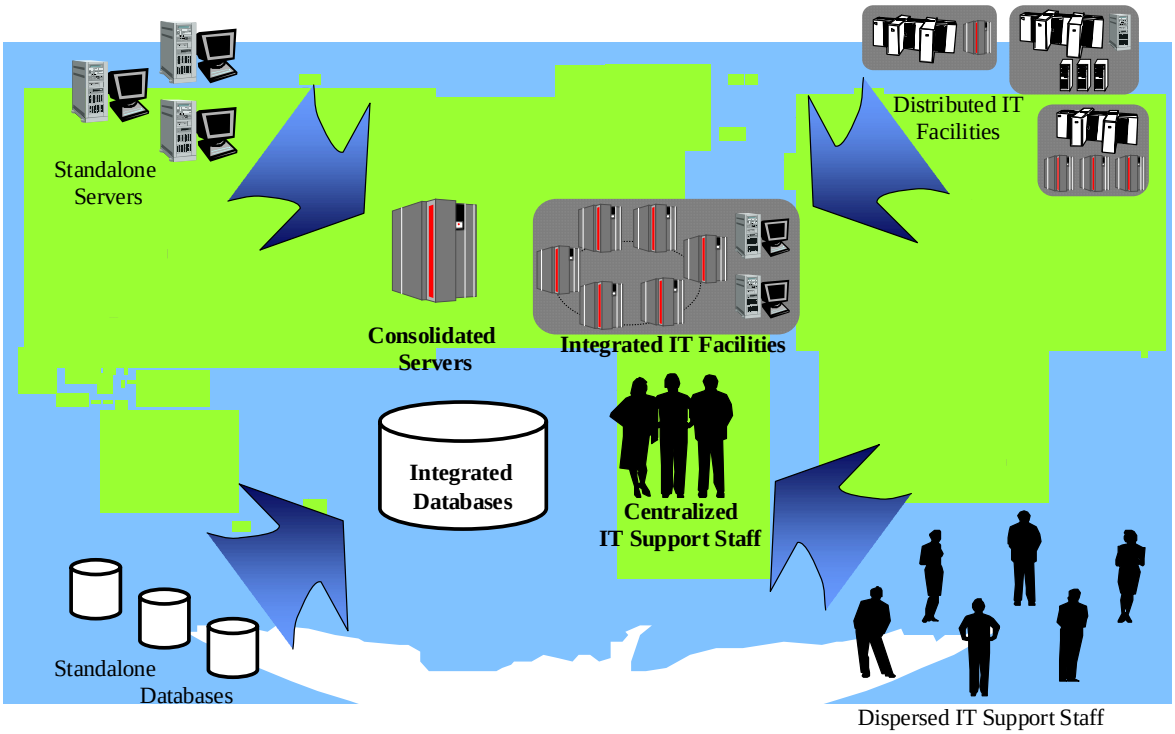
The USG has rules and procedures governing how financial, procurement and other administrative transactions may be carried out. The program for re-inventing government has already changed many of these procedures. However, remaining USG requirements may inhibit the prompt achievement of this objective.

Objective 4B - Consolidation of Information Technology Facilities

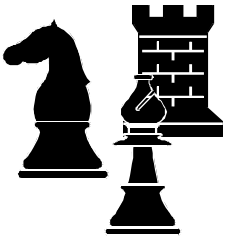
The Department operates many computer/ communications centers on a worldwide basis. In large measure these separate facilities were established at a time when slow-speed, unreliable communications made it imprudent for remotely located users to rely on international communications circuits to provide required access to computers. *As these communication capacities are extended through the implementation of commercial global networks, the Department will be in a position to provide regional or central computer support via high-speed communications lines to geographically distributed users,* and to do so at a lower cost than that required for staffing and maintaining separate computer facilities at each user location.

This objective is focused on reducing complexity, and subsequently constraining costs, by minimizing the number of separate computer/ communications facilities operated by the Department. Databases will be consolidated where practical, and corporate applications will be supported via larger, shared servers housed in central facilities. Additional benefits will be improved security, data integrity, operational reliability, technical support, and availability.

With the achievement of this goal, the Department will be able to support increasingly complex IT activities with its limited pool of highly skilled technicians.



Means and Strategies



The Department has already successfully consolidated a number of overseas computer and communications facilities. It has also consolidated a number of domestic computer facilities in its Combined Bureau Processing Centers (CBPC). Through this program ***most*** Bureaus have co-located their computer servers in a few secure facilities that are staffed to operate around the clock.

The Department will continue to consolidate its major application databases into as few facilities as possible. Whenever possible, systems will be consolidated at centralized communications facilities, thus enabling the sharing of technical talent and the reduction of facility and overhead costs. The results of ongoing capacity management studies will be analyzed to determine the best placement of computing support centers across the enterprise. These studies are currently focused on the network capacity, but will be expanded to include capacity requirements for servers. The results will show the Department how best to consolidate multiple applications and databases on corporate, shared platforms.

With the availability of commercial style networking, the Department's modern mainframes are already available to be used as corporate super-servers for applications, messaging and web services. Additionally, they enjoy a high level of availability, reliability, and scalability. These super-servers will be exploited to the maximum extent possible to support a wide range of centralized client-server and web-based applications.

The knowledge base built by the Department's well-established Data Administration program will be the foundation for analysis to begin consolidating and integrating databases. The Department will apply modern techniques in database and information management to ***consolidate and integrate key corporate databases***. For example, the Department will field a fully integrated human resources (HR) database, covering all personnel and all HR transactions.

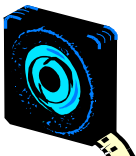
*Posts will continue to have an IT point of presence, but most data and processing will occur at **consolidated locations**.*

This consolidation of data and systems will enable the Bureaus to concentrate functional support staff. While the facilities will be operated by the central IRM organization, Bureaus will enjoy the ability to place technical staff within the core facilities as well as access their systems and data remotely for content and administrative management. This arrangement will enable the Department to matrix and leverage highly skilled technical resources, thereby reducing skill and workload overlap and redundancy across the enterprise.

Major Milestones

Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured



FY2001

- Plan and schedule for consolidating overseas servers

FY2002

- All classified Bureau servers (except S/S, INR) located in server farms
- Integrated mainframe parallel sysplex established linking Main State and BIMC dynamically

Output
- % of classified computers in server farms

Outcome
- Reductions in numbers/costs of domestic IT technicians

FY2003

- All unclassified Bureau servers (except S/S) located in server farms
- Corporate web-based applications consolidated on mainframe super-server

Output
- % of unclassified computers in server farms

Outcome
- Reductions in numbers/costs of overseas IT technicians

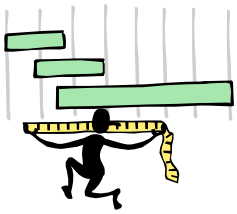
FY2004

- All classified Bureau servers (except S/S, INR) located in server farms

Output
- % of countries serviced by consolidated centers

FY2005

- Overseas server consolidation completed as planned



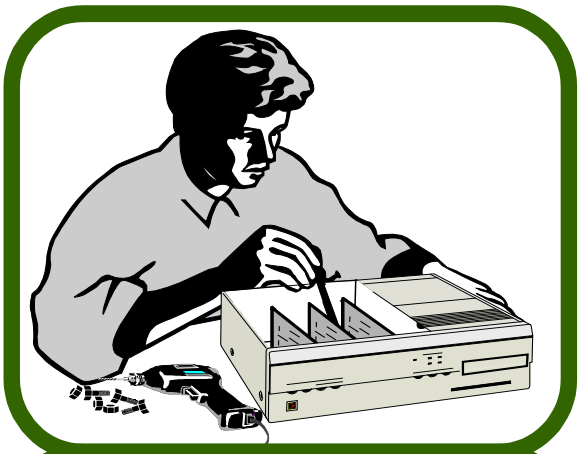
External Factors

Other than the availability of funding, there are no external factors that will have a substantial impact on the achievement of this objective.

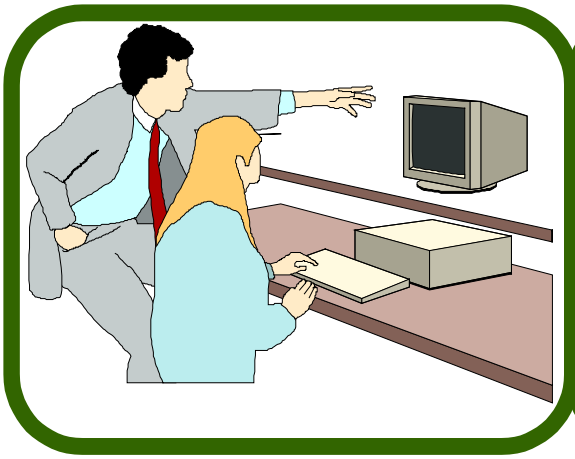
Goal 5 - Sustaining a Trained Productive Workforce

As indicated previously, the Department plans to control its worldwide requirements for IT specialists by consolidating the number of computer/communications centers that must be supported. It also plans to reduce worldwide requirements for administrative personnel by streamlining procedures, simplifying and consolidating systems, and taking the fullest advantage of electronic technology to perform required administrative functions.

Consistent with OMB and congressional dictates, the Department plans to outsource commercial-type technical and administrative functions, where cost, operational, and security considerations make that approach feasible. This will enable the Department to support its steadily growing technical needs and its administrative support requirements within expected resource constraints.



However, the ability to accomplish more work with no more people in an increasingly complex technical environment depends on establishing and maintaining high levels of skill and training for that workforce. This goal addresses the requirement for ensuring that the in-house cadre of Department IT specialists and the wider Department population of hardware/software users are fully capable of carrying out their responsibilities effectively.



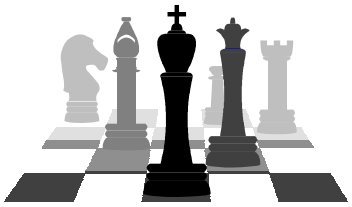
Objective 5A - A Rewarding Workplace For IT Specialists

The Department has difficulty attracting and keeping a highly qualified technical workforce capable of providing world class support to its far-flung operations. Like most USG agencies, the Department faces serious impediments in attracting and retaining such professionals. Its pay scale is not competitive with that of industry. Its requirement for a full background security clearance makes its recruitment efforts more problematic. Its career paths for IT specialists are limited and for the Foreign Service include worldwide assignment availability. Its technical working environment is not at the forefront of the industry. All of these impediments, taken together, seriously impact the ability of the Department to build the information technology workforce it needs.

This objective is directed toward upgrading the quality of the Department's IT workforce on a long-term basis by establishing working conditions that will serve to attract and keep the highly qualified professionals needed.

Achievement of this objective will have significant benefits. The Department's IT specialists will receive competitive pay for their work and will enjoy career opportunities that do not now exist. And the Department, in turn, will gain a higher quality IT workforce.

Means and Strategies



The Department plans to attract and retain qualified IT specialists by reducing impediments to their recruitment and by providing a rewarding working environment for them once they are on board. Recruitment bonuses have already been instituted and retention incentives have been proposed. These measures, combined with careful outsourcing for IT skills not unique to the Department, should provide the Department with the IT skills pool it requires. In particular, it plans to:

- Implement the IT Training Plan which specifies appropriate training for all Civil Service and Foreign Service IRM personnel. The plan is based on the Department's business requirements as set forth in the Department's Strategic Plan, and the IT Strategic and Tactical Plans. It will provide appropriate technical and managerial training for IRM personnel, including courses leading to certification.

- Establish an unclassified computer laboratory at the Foreign Service Institute that will focus on advanced techniques applicable to Department operations, such as: PKI; S/MIME; and web-based technologies (particularly search engines and web portal techniques).

- Work through OPM and the Chief Information Officers Council to establish special pay provisions for qualified IT specialists.

- Establish and operate a certification program for Department employees that, based on both technical knowledge and technical accomplishment, will enable them to qualify for special pay.

- Expand the personnel resource base to provide the flexibility needed to release employees for required technical training.

- Identify key technical positions that can only be filled by certified IT specialists.

- Establish career paths for IT specialists that permit them to seek advancement not only to the top technical jobs in the Department, but also to top administrative / management positions, both domestically and at overseas posts and regional centers.

Major Milestones

FY2001

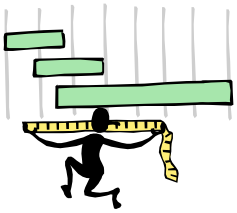
- Advanced computer laboratory established at FSI
- Pre-employment security clearance process for top-quality IT specialists accelerated

FY2002

- New career ladder for IT specialists established
- Opportunities for state-of-the-art IT activities created

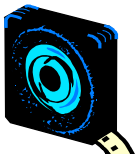
FY2003

- Certification procedures for Department IT employees implemented
- Competitive compensation for IT employees put in place



Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured



Output

- Cumulative number of certified IT specialists (recruited from outside the Department) still on board

Output

- Cumulative number of certified IT specialists (certified from Department ranks) still on board

Outcome

- Total number and salary costs of Department IT specialists

External Factors

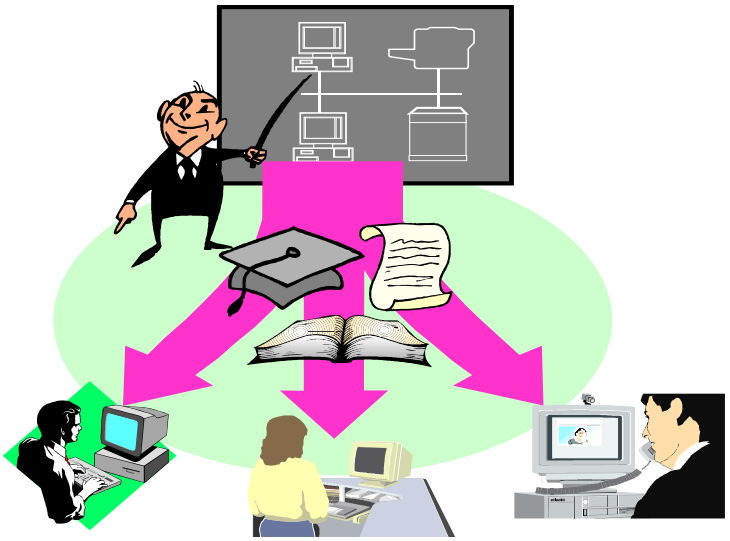
An important external factor that will affect the ability of the Department to achieve this objective is the willingness of the USG to authorize special pay for IT specialists.

Objective 5B - An Effective Distance Learning Program

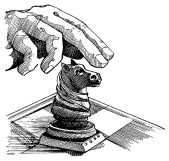
Most private enterprises and government agencies have a serious problem in maintaining the training level of their workforce at a high level, given the rapidly changing technological environment that characterizes today's workplace. The Department faces a particularly difficult problem in this regard because of the geographically dispersed, multinational character of its workforce.

This objective is directed toward maintaining a high level of training for Department employees throughout the world by means of modern distance learning techniques, including the use of videoconferencing.

Achievement of this objective will have significant benefits. The Department's employees will have opportunities to increase their skills and advance their careers. As a result, the Department will have a higher-quality workforce that is more capable of fulfilling its mission requirements than is today's workforce.



Means and Strategies

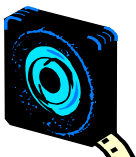


The Foreign Service Institute (FSI) is widely recognized for the quality and variety of the instruction it provides to Department and other USG employees. Among its courses are approximately 50 pertaining both to technology, in general, and to specific hardware and software systems. Most of FSI's instruction takes place at its campus in Arlington, Virginia. However, during the past several years FSI has provided instructors to the ALMA teams that has installed modern equipment and systems on-site at Foreign Service posts. The Department plans to achieve its IT training objective by building on existing FSI capabilities and, in particular, making FSI course content available to Department employees on a worldwide basis through advanced communications.

For some courses this means restructuring course content for use with computer-based training (CBT). In this situation, students will be able to download courses for study on their own desktops during times of their choosing.

For other courses, in which interactive participation is beneficial, the Department plans to use full motion videoconferencing, so that instructors and students can operate in a virtual classroom setting, even though they may be separated by thousands of miles.

Major Milestones



Performance Measures

Performance measures for this objective are identified below during the first year in which they are measured

FY2002

- ⌂ Full range of IT courses provided through distance learning

FY2003

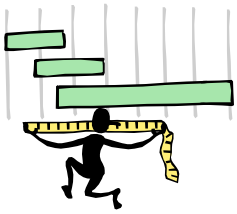
- ⌂ Interactive training provided through multi-point videoconferencing
- ⌂ Course material reviewed and updated*

Output
- Number of courses available through distance learning

Outcome
- Number of courses completed through distance learning

Output
- Number of courses available through videoconferencing

Outcome
- Number of courses completed through videoconferencing



* Milestone recurring annually

External Factors

Other than the availability of funding, there are no external factors that will have a substantial impact on the achievement of this objective.

This Page Intentionally Left Blank

STRATEGIES for ACHIEVING IT GOALS and OBJECTIVES

Strategies for achieving specific IT objectives have been described in the previous chapter. This chapter addresses broader strategic principles that apply to at least several, if not all, the IT objectives set forth in this Strategic Plan.

Management Strategies

The Department plans to adopt the following management strategies in implementing this Strategic Plan:

- Proceed with projects only after appropriate studies have been completed and the results of these studies have been reviewed by the Capital Planning review groups set up for that purpose (requisite studies include: business process re-engineering studies; functional requirements specifications; analyses of alternatives; and cost/benefits analyses);

- Begin these requisite studies during 2000, so that project development work can proceed during 2001, followed by extensive pilot testing in 2002, and worldwide deployment in the three subsequent years covered by this plan;

- Conduct management reviews of ongoing projects on a quarterly basis and authorize continuation of projects at various gates defined in Managing State Projects (MSP) procedures;

- Insist that project sponsors limit requirements to those that can be met by commercially successful COTS packages;

- Outsource IT projects whenever it makes sense to do so (e.g., seat management);

- Apply the principles of risk management, rather than risk avoidance, in determining the applicability of security measures to be used in protecting the Department's IT systems and facilities;

- Work closely with other agencies to carry out the OPAP recommendations and ensure effective interagency connectivity and information sharing;

- Centralize enterprise-wide IT funding through the Central Fund to provide necessary resources to operate the infrastructure; and

- At the beginning of the 2001-2005 period allocate approximately 50% of the Central Fund to projects that implement this Strategic Plan, and gradually increase that percentage over the five-year period.

Technical Strategies

The Department plans to adopt the following technical strategies in implementing this Strategic Plan:

- Base the Department's IT environment on the web in the following ways:
  - Achieve any-to-any communications connectivity needed that cannot be provided by USG networks;
  - Emulate the "look and feel" of the web for the Department's applications;
  - Adopt software and facilities that have proved successful on the web; and
  - Adopt the de facto access, data, and applications standards of the web.
- Maximize the use of COTS packages;
- Coordinate technology solutions with other agencies in the international affairs and intelligence communities, minimizing duplication of effort and promoting interoperability and efficient technical support;
- Require IT projects and systems to conform with the Department's IT architecture and standards;
- Require independent verification and validation (IV&V) and pilot tests of all IT systems before deployment;
- Conduct a joint pilot test (prospectively during 2002 at the seven Foreign Service posts in Canada) of all IT projects undertaken to implement this Strategic Plan; and
- Deploy on a unified basis the operational capabilities developed, but only after their effectiveness have been demonstrated in an operational test environment.

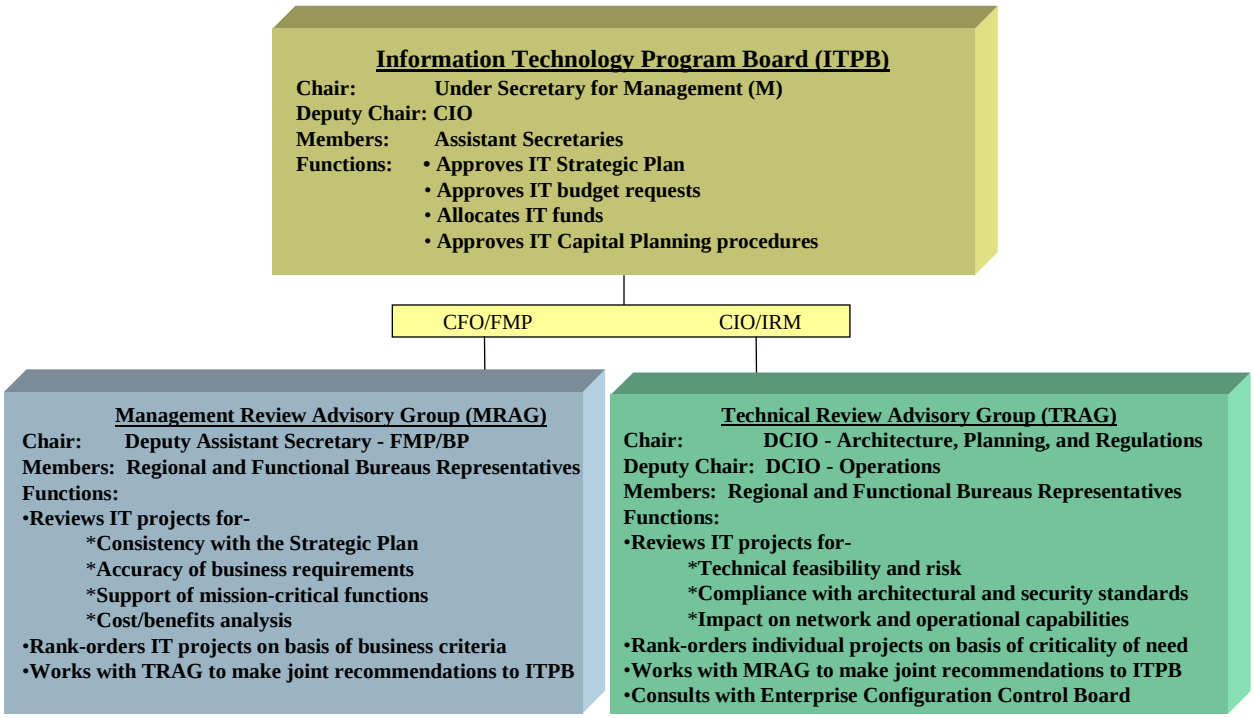
IT MANAGEMENT and PLANNING PROCESSES

Management – In 1996 the Department established an IT Capital Investment Fund (CIF), along with a management group, headed by the Under Secretary for Management, to determine how best to apply CIF resources to meet the Department's objectives. In recent months the Department has re-structured this mechanism to meet the requirements of OMB Circular A-11 for IT Capital Planning.

Under this new arrangement the senior management group, the Information Technology Program Board (ITPB), approves the IT Strategic Plan and advises the Under Secretary for Management on funding allocations for the Department's IT activities. Members of the ITPB are at the Assistant Secretary level and represent the Department's regional, functional, and management bureaus.

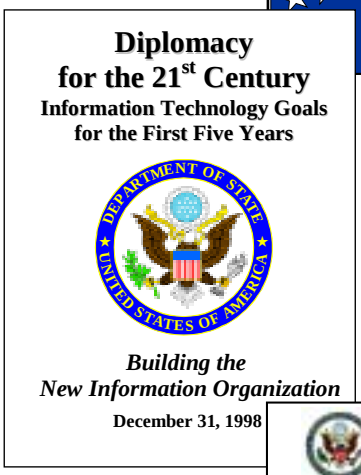
The ITPB is supported by two advisory groups: 1) the Management Review Advisory Group (MRAG) that evaluates the investment potential of IT projects and their ability to support the Department's IT Strategic Plan; and 2) the Technical Review Advisory Group (TRAG) that assesses on an on-going basis the technical merits of IT projects, their conformance with IT architectures and standards, and their potential impact on the Department's communications networks and on its overseas operations.

IT Capital Planning Process



Together, the ITPB, MRAG, and TRAG ensure that IT projects and systems:

- Support the mission of the Department of State;
- Represent sound investments;
- Are carried out in the most cost-effective manner possible; and
- Present low technical risk.

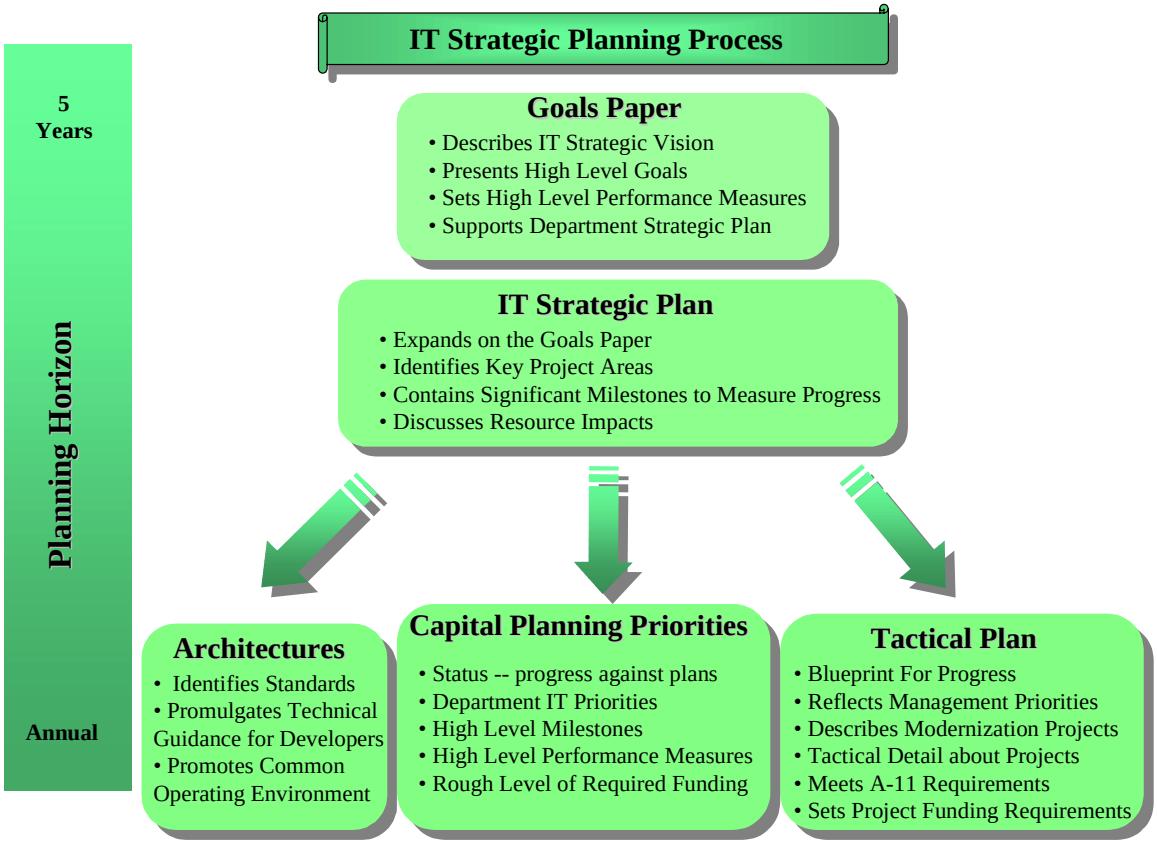


Planning – The Department's planning structure is headed by the Office of Management Planning (M/MP), which is responsible for coordinating the International Agencies' Strategic Plan and for producing the Department of State' Strategic Plan, along with Annual Performance Plans.

Before approving the IT Strategic Plan, the ITPB ensures that it fully supports the Department's overall Strategic Plan. Following approval, the ITPB uses the IT Strategic Plan as a guide for allocating available resources to IT projects and systems. Projects approved by the ITPB are described in the IT Tactical Plan, which is published on a semiannual basis. The most recent version of the IT Tactical Plan includes nearly 100 project descriptions. However, in the next edition that number will grow, as IT projects supporting the work of ACDA and USIA are added.

As the Department proceeds to implement this new version of the IT Strategic Plan, its mix of IT projects is expected to change substantially. The current Tactical Plan projects will be reviewed to ensure their fit with this new IT Strategic Plan, which in turn is based squarely on the precursor IT Goals Paper, that was reviewed thoroughly over a six-month period and received Department-wide concurrence. This document has been produced with input provided by most of the Department's bureaus and with review and concurrence by all of them. It has been approved for publication by the ITPB. It is a valid reflection of the Department of State's IT strategic goals and objectives for the 2001-2005 period.

The figure below shows the relationships among the Department's strategic goal setting and planning processes and its tactical planning and related activities. The strategic goals, specified first in the IT Goals Paper and now in this IT Strategic Plan, have a long-range planning horizon – up to five years. These documents are linked directly to the Department's mission-oriented Strategic Plan. The strategic IT goals and objectives drive shorter term tactical and operational decisions and project plans. They are the basis for architectures, planning and budgeting priorities, as well as the annual Tactical Plan. The process enables management to make investment decisions that focus resources on mission needs and strategic priorities and directions.



This Page Intentionally Left Blank

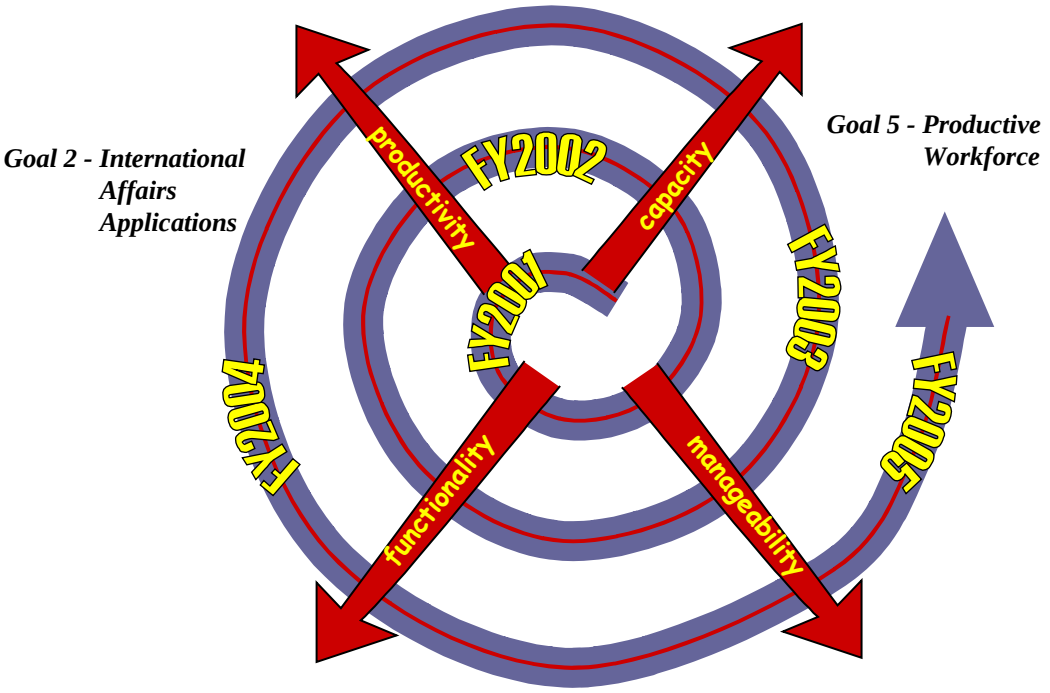
PRIORITIES AND DEPENDENCIES

The five strategic IT goals described in this document are of several different types. Goals 2 and 4 identify business outcomes in international affairs and administrative support that the Department seeks to achieve. Goals 1 and 5 address the infrastructure improvements in IT equipment and human resources that the Department must have to be able to achieve the desired business goals. Goal 3, an integrated messaging system, can be considered to include both business and infrastructure elements. The Department's top IT priority is the direct support of substantive functions that are central to its mission - that is, the international affairs activities addressed by Goal 2. The highest priority for IT is the support of these mission functions through improved diplomatic readiness – a category that includes a range of infrastructure, management, and administrative support functions addressed by the other four goals. To achieve diplomatic readiness, the Department must concentrate on and invest in critical infrastructure elements (Goals 1 and 3) that exist only to support the Department's business objectives.

Modern messaging technologies will provide a foundation for mission and administrative operations

*If we don't implement a **high capacity scalable network now,** we will not succeed with the critical mission-support and diplomatic goals.*

Goal 1 - Networks and Infrastructure



Goal 2 - International Affairs Applications

Goal 5 - Productive Workforce

Goal 3 - Integrated Messaging

Goal 4 - Streamline Operations

The goals and objectives are mutually interdependent on one another and must be pursued in close coordination, if the broad aims of this strategic plan are to be achieved. Clearly, the infrastructure objectives are foundational, and the Department is committed to establishing the robust global infrastructure projected under Goal 1.

However, work on all goals and objectives will proceed iteratively and in parallel. The Department will proceed rapidly to improve, re-engineer, strengthen, and implement capabilities and capacities. At the same time we upgrade foundational network facilities around the world – a multi-year initiative – we will begin pilot and production deployment of collaborative processing, modern messaging components, administrative solutions, and other non-infrastructure solutions. The nature of modern IT is that solutions must be designed and deployed in modular increments, ensuring flexibility and ability to capitalize on industry directions and emerging and evolving Department requirements. Design and development will be iterative as new and upgraded technologies are integrated into previously established systems.

Thus, we will deliver infrastructure, functional, management, productivity and capacity improvements in increments and in parallel.

The IRM Planning Division will produce a paper that establishes a more detailed analysis of dependencies, investment priorities, and critical path. This paper will analyze existing projects and identify required projects to ensure their compatibility with this Strategic Plan. It will also detail the needed critical infrastructure initiatives (e.g., network, messaging) that are essential for supporting the mission critical diplomatic goals.

ESTIMATED COSTS

The estimated costs for implementing this IT Strategic Plan will be based on the Department's past experience in deploying and operating IT systems on a worldwide basis. The accuracy of these estimates is considered appropriate for this point in the planning process: they indicate an expected order of cost magnitude for carrying out this Plan. As it proceeds to conduct cost/benefits analyses for the strategic IT objectives, the Department will improve on the accuracy of the initial cost estimates and begin projecting long-term savings and/or cost avoidance in some areas as a result of implementation of this Plan.

The incremental development approach described in the preceding chapter will be the basis for the cost estimates. Much work will be done in parallel, and some work will begin immediately on all five goals. Most required preliminary studies (e.g., BPRs, benefit/cost analyses) will be completed during FY2000 and FY2001, and design, pilot testing, and initial deployment will proceed in parallel to the maximum extent possible.

Cost estimates for each goal will be developed over the next six months and will be based on industry benchmarks and best practices. Estimates will also be based on a critical path model that reflects critical dependencies among goals, objectives, and specific initiatives needed to accomplish objectives. The figure on the following page shows whether costs are expected to increase, decrease, or remain the same as current levels for each goal and each year. For Goal 1, for example, costs will increase in the first two years, as major investments are made to modernize and upgrade the global network and infrastructure services. Once a commercial-style infrastructure is in place, beginning in FY-2002, costs will decrease in relation to today's costs.

Anticipated Funding Increases/Decreases over the Five-year Period Needed For the IT Strategic Plan

GOALS	FY-2000	FY-2001	FY-2002	FY-2003	FY-2004	FY-2005
1. A Secure Global Network and Infrastructure	+	++	-	--	-	=
2. Ready Access To International Affairs Applications and Information	+	++	++	+++	+++	+++
3. Integrated Messaging – A Worldwide Approach	+	+	+	+	=	=
4. Leveraging IT To Streamline Operations	++	++	+	-	-	=
5. Sustaining A Trained Productive Workforce	+	+	+	+	+	=

The objectives specified in this plan are aimed at improving the conduct of business while avoiding potentially significant cost increases in the future. The Department sees its first priority as increasing the effectiveness of our support for the diplomatic mission, but also seeks opportunities for cost containment through use of technology, re-engineering, consolidating business processes, and centralizing some operations. These cost containment opportunities can be achieved only if we first make significant investments in our global IT infrastructure. For example, streamlining operations through consolidation is possible only after we have a secure, robust network in place. Modernized business and messaging applications will yield efficiencies and savings, but are dependent on up-front investments, first in infrastructure and then in specific technology solutions. The Department is therefore committed to a ***comprehensive approach to lowering total life cycle costs***, rather than focusing on initial costs or merely addressing cost issues year-by-year. We are convinced that the Department is on a path that will yield efficiencies and cost containment, while also increasing the effectiveness of IT systems and diplomatic readiness.

The Department anticipates significant cost avoidance by implementing the objectives outlined in this plan. However, these results will not be fully enjoyed for several years, and the Information Technology requirements associated with modern diplomacy will likely increase over the next few years. Two recent studies conducted by prominent diplomatic experts discuss the radical changes expected to occur in the conduct of diplomacy and international affairs[2]. These changes include a demand for far greater connectivity with other countries, NGOs, and various publics than we have today. Security requirements will likewise increase, as will demand for infor-

[2] The Stimson and CSIS reports

mation access, intelligent analytical tools, powerful search engines, and other technologies. The Department is committed to supporting our diplomats as we move into this new age. We are seeking to establish a robust IT environment that will support ***e-Diplomacy –*** the conduct of diplomacy in the age of the Internet and other technological advances. The Overseas Presence Advisory Panel (OPAP) has issued draft recommendations calling for State to assume responsibility for extending this robust, standardized IT infrastructure to support the entire international affairs community – thus extending the benefits of e-diplomacy to all agencies with a role in international affairs. Clearly, this will require significant investments over the next few years. We must continue to make the investments needed to support the vision presented in this plan and add value to the conduct of international affairs by:

- ***Building a robust networking and security infrastructure*** – To address the challenges and build the global network we need, we must address PDD-63 and a number of security concerns, some of which are unique to the Department's position and role as the lead international affairs agency. Our systems are vulnerable to internal and external threats. Our overseas posts are heavily dependent on foreign nationals. As communications capabilities increase, so do the security threats and risks associated with unauthorized access to sensitive information. As we connect our networks to the Internet, we must be sure to protect the integrity of our information assets. Accordingly, there are significant investments still to be made, including continued replacement of an aging and obsolete communications infrastructure and establishment of standardized security services needed to support the diplomatic mission. ALMA has made significant strides to address the overseas unclassified component; we must now turn our attention to the domestic and worldwide-classified components.

- ***Providing ready access to international affairs information and applications*** – The Department will face significant challenges to implement this goal. As noted in this Plan, much of the resources in the past have been steered towards administrative systems. The substantive systems are lacking – we must invest funds in studies to re-engineer the way business is conducted. We must then design, test, and implement the new systems and databases that will assist the substantive users in searching, acquiring, and manipulating the vast amounts of information required to conduct foreign policy in this new era. We will pursue solutions that rely on and mimic commercial technologies, such as the Internet, giving political and economic officers familiar web-based access to information and the electronic tools to process it. We will provide powerful, intelligent search systems to aid people in identifying and retrieving information from a wide range of sources. To pursue e-diplomacy in the new millennium, we can afford to do no less.

- ***Building a robust messaging system*** – Our existing formal messaging system and infrastructure is obsolete and must be totally replaced. Furthermore, the business processes that it currently supports are equally

arcane and must be re-engineered. There is a significant amount of work ahead of us to conduct BPRs and fully replace the existing systems. We will invest in new technology, to be sure, but we will also modify the ways in which the Department moves information around, shares information internally and externally, and stores and retrieves information. The end result will be a modern approach to information management and exchange focused on the conduct of international affairs. All of this will require significant investment in infrastructure, technology, process engineering and design, training, and human resource management.

- ***Streamlining and consolidating operations through IT*** – A global network and modern application and data management tools will enable the Department to consolidate activities that are currently performed at numerous locations around the world. Examples include logistics, personnel functions, and financial management. The complex IT environment of the modern world demands high levels of management and support. Through this initiative, we will be able to consolidate the overseas and domestic support structure, achieving economies of scale and improved service. However, we must in many cases re-engineer existing applications and databases and then implement new web-based systems that will enable us to centralize operations. In addition, regional facilities may have to be constructed, or modernized and restructured, to support the new vision presented in this Plan. We will make increasing use of modernized mainframe technology and powerful database management approaches, including data warehouses, web-based data systems, and active management of database and system interfaces. All of this will require financial and personnel resources.

- ***Sustaining a trained workforce*** – We have extraordinary personnel costs associated with supporting our worldwide infrastructure. The Department is highly decentralized, and our overseas posts have important and demanding requirements for timely and reliable information systems support. Accordingly, we must deploy highly skilled technical staff at remote locations, greatly increasing costs. Like many organizations, our turnover among IT staff is high, and we are faced with the need and costs of ongoing training. Furthermore, we must expend resources to develop the new training courses and techniques described in this plan. Recruiting and retention are critical issues, and we must make the investments needed to sustain the best workforce possible.

Once we institute the planning and management processes described in preceding chapters, we will be able to implement the goals and objectives presented in this Plan. This in turn will enable us to streamline and simplify operations and begin to contain costs. We should then see the Department's IT budget level off and perhaps begin to decline as a percentage of total budget. However, even after we succeed in lowering some costs, we still face the following major challenges that may affect our overall resource requirements:

- **Continued support for more than 230 overseas locations around the world** – The high costs for networking, security, staff support, training, can be mitigated, but must be met. Additionally, we must continually adapt to an ever-changing political and economic world, which may require opening and closing of Embassies, Consulates, and other facilities worldwide.

- **Extraordinary security, reliability, and contingency requirements**, requiring multiple networks and computers for most staff, secure telephones, emergency radio equipment, satellite communications, and redundant backup facilities. Because of security requirements, the Department will continue to operate two complete global networks and infrastructures (classified and unclassified) – a very complex and expensive undertaking. We cannot afford to skimp on security.

- Support for travel of the President, Secretary of State, members of Congress, and foreign dignitaries, which places large demands on our IT resources. Here again, we cannot afford to fall behind in our investments and risk catastrophic failure.

- Support for special Congressionally mandated programs, such as Embassy security, for which we are investing large sums to upgrade emergency and evacuation networks; and border security, for which we are investing many millions of dollars for the visa and passport modernization and Border Crossing Card programs. The cost of these programs often increases because of a combination of tight deadlines, the need to cooperate with other agencies and nations, and the requirement for cutting edge technology widely distributed around the world. Life cycle maintenance and support must also be taken into consideration.

In summary, we firmly believe that this Strategic Plan will lower the total life cycle costs of many Departmental systems. At the same time, we recognize that the conduct of international affairs is highly dependent on timely and accurate information. It takes resources to access and analyze that information. The nation runs a grave risk if we fail to provide our overseas staff with ready access to the information they need to make informed decisions and provide the excellent analyses and advice the Department's decision makers depend on. We can not afford to fall any further behind in IT. Accordingly, we must finish the job of modernization, while properly addressing PDD-63 infrastructure protection issues and positioning the Department to engage in *e-diplomacy*. In order for the Department to achieve these ambitious goals, its IT budgets will probably have to remain relatively high for the next few years.

This Page Intentionally Left Blank

Acknowledgements

Fernando Burbano, the Chief Information Officer (CIO) of the Department of State, would like to acknowledge the effort put forth by members of IRM/APR/IAP/PL and by the other persons listed below in preparing this IT Strategic Plan.

IRM/APR Staff

Henry Allison – IRM/APR/IAP/PL
Kenneth Alms***** – IRM/APR/IAP/PL
Barry Finkelstein – Finkelstein Consulting, Inc.
Paul Fisher – IRM/APR/IAP/PL
Wally Francis – Consultant
Donald C. Hunter***** – IRM/APR, Deputy Chief Information Officer
John Lemandri – IRM/APR/IAP/PL
Grant Lorenz – J.G. Van Dyke and Associates
Tim McAndrew – J.G. Van Dyke and Associates
Kelly Peters – J.G. Van Dyke and Associates
Karl Sanger – Consultant
Ron Somerville – Consultant
Andy Tainter – J.G. Van Dyke and Associates

Contributors

Dave Ames – IRM/Y2K, Deputy Chief Information Officer
Bert Edwards – Chief Financial Officer
Larry Eisenhart – Deputy Chief Financial Officer
Todd Greentree – S/RPP
Patrick Kennedy – Assistant Secretary of Administration
Bruce Morrison – Foreign Service Institute
Frank Moss – Executive Director, Bureau of Consular Affairs
Lloyd Pratsch – A/OPE. Procurement Executive
Dan Sheerin – IRM/EX/PAS
Steve Shinnick – Bureau of Administration
Robert Surprise – IRM/OPS, Deputy Chief Information Officer
Ruben Torres – Executive Director, Bureau of Personnel
Ambassador Andrew Winter

***** *If you have questions or comments concerning this paper, please contact the IRM/APR staff indicated above.*

This Page Intentionally Left Blank

APPENDIX A

GLOSSARY

A-11	Office of Management and Budget Circular that prescribes planning, budgeting and acquisition procedures for USG agencies.
ACDA	The Arms Control and Disarmament Agency, which has now been consolidated with the Department of State.
ALMA	A Logical Modernization Approach - Department model for managing automated information systems and telecommunications modernization efforts based on use of Information Technology (IT) standards and commercial products.
Bandwidth	Used to identify, or 'measure' the capacity of a telecommunications circuit or local area network (LAN).
BIMC	Beltsville Information Management Center.
BPR	Business Process Re-engineering.
BRN	Black Router Network. A DTS-PO IP-based network in pilot phase – The "Intranet" of the Foreign Affairs Community.
CA	Bureau of Consular Affairs.
CableXpress	An automated system that delivers cables and e-mail to the desktops of users.
CBPC	Combined Bureau Processing Center.
CBT	Computer-based Training.
CF	Central Fund - the Department's primary source of funds for IT development.
CFO	Chief Financial Officer.
CIF	Capital Investment Fund – a major part of the Central Fund.
CIA	Central Intelligence Agency.
CIO	Chief Information Officer.
Class Net	Department IP-based network able to handle information up through the Secret security level.
CM	Configuration Management.
CMOS	Complimentary Metal Oxide Semiconductor.

GLOSSARY

COE	Common Operating Environment. A term used to refer to a specific configuration for platforms such that all users utilize the same configuration thereby lowering management and troubleshooting effort and costs.
COTS	Commercial, Off-The-Shelf. Refers to readily available commercial products requiring no development.
DART	Delay, Availability, Reliability, Throughput. Network performance measures.
DoS	Department of State.
DS	Bureau of Diplomatic Security.
DTS-PO	Diplomatic Telecommunications System Project Office – the organization responsible for acquiring overseas communications capabilities for USG agencies.
E-diplomacy	The new multi-faceted diplomacy in an electronic age as documented in the recent Stimson and CSIS reports. To be effective in the next century, our diplomats will require access at their fingertips to a wealth of information and effective tools to manipulate that information and share it with others. To keep up with the issues of the day, they will require Internet-like networks and intelligent automated agents that can help them find and organize critical information. They will need ability to collaborate with counterparts in other agencies, foreign governments, non-governmental organizations, and the public. Their work will become increasingly dependent on information and IT networks.
EB	Bureau of Economic and Business Affairs.
Encryption	The use electronic coding techniques to protect information from disclosure to unauthorized readers, to prevent undetected modification of the information, and to support reader to writer identification and authentication.
ERP	Enterprise Resource Planning.
FAA	Federal Aviation Administration.
Firewall	Any telecommunications or network device used to regulate/control the flow of information packets between networks. The firewall, or firewalls, implement an IT security policy by screening information to verify that it complies with policy, do not contain malicious code, and are not otherwise attempting to intrude on the protected network side or disrupt its operations.
FSI	Foreign Service Institute – the Department organization responsible for employee education and training.
FTP	File Transfer Protocol.

GLOSSARY

FY	Fiscal Year.
Groupware	Software designed to facilitate the efforts of a group, typically with a common interest or goal – often used to support brainstorming, consensus building, or other activity involving the free flowing exchange of ideas and information among several individuals at the same time.
GSA	General Services Administration.
HR	Human Resources.
INR	Bureau of Intelligence and Research.
Intranet	An internal IP network using the same information transfer methods and device connection types as the Internet. Open Net and Class Net are the "Intranets" of the Department.
IP	Internet Protocol - the basic standard established for data exchange over the worldwide Internet and widely adopted by organizations operating private networks, such as the Department's Open Net and ALMA-based LANs.
IRM	Information Resources Management – the Department organization responsible for managing information technology.
I&A	Identification and Authentication – The process and means of validating the identity of an authorized user.
IT	Information Technology.
ITA	Information Technology Architecture.
ITPB	Information Technology Program Board.
ITRMS	IT Resource Management System.
IV&V	Independent Verification and Validation.
LAN	Local Area Network. A small network that serves a group of users. Typically confined to a single facility. Most LANs in the Department are built using Ethernet (10BaseT) hubs.
M/MP	Office of Management Planning.
MLS	Multi-Level Security. A computer security methodology whereby systems approved for the storage and processing of information of differing sensitivity levels simultaneously permit access by users with different security clearances and needs-to-know, and prevents users from obtaining access to information for which they lack authorization.

GLOSSARY

MRAG	Management Review Advisory Group. This group is chaired by the Deputy Assistant Secretary for Management and evaluates the investment potential of IT projects and their ability to support the Department's IT Strategic Plan.
MSP	Managing State Projects. A DoS project management methodology.
NGO	Non-Governmental Organization.
NSA	National Security Agency.
OMB	Office of Management and Budget.
OPAP	Overseas Presence Advisory Panel.
Open Net	Department IP-based network able to handle information up through the Sensitive But Unclassified level.
OPM	Office of Personnel Management.
Out-of-band	Used to refer to the conduct of an event outside the normal bounds of communications.
PA	Bureau of Public Affairs.
Parallel sysplex	Refers to a particular configuration of computing resources wherein multiple processors are arranged in parallel to increase processing speed and power.
PC	Personal computer.
PDA	Personal Digital Assistant.
PDD	Presidential Decision Directive.
PKI	Public Key Infrastructure. The term used to refer the system required to supply and manage certificates for public key encryption and digital signature used by clients and servers.
Platform	In the context of this document, the platform is the stable, cross-project base of both hardware and infrastructure software provided to (and evolved for) all projects in the Department. Note that this contrasts with some commonly held definitions that consider "platform" to include only the hardware base.
Protocol	A defined structure, contents, and flow for communications between computers and other networked devices.
Push and pull	Used to describe two discrete methods of information dissemination. The "owner" of an information resource may "push" information to one or many recipients. Conversely, "pulling" information involves a consumer accessing a common information resource and withdrawing the item of choice.

GLOSSARY

S/MIME	Secure/Multipurpose Internet Mail Extension. Provides a consistent way to exchange secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). S/MIME is used by traditional mail user agents to add cryptographic security services to mail that is sent, and to interpret cryptographic security services in mail that is received. However, S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP. As such, S/MIME takes advantage of the object-based features of MIME and allows secure messages to be exchanged in mixed-transport systems. Further, S/MIME can be used in automated message transfer agents that use cryptographic security services that do not require any human intervention, such as the signing of software-generated documents and the encryption of FAX messages sent over the Internet.
S/S	Executive Secretariat.
SAS	State Archiving System.
SDE	Standard Data Element. Agreed upon convention for defining elements of information.
Seamless	Used to describe the relative ease or difficulty associated with the transfer of information across application or system boundaries. Copying text from a document and pasting it into a database is effortless in an integrated, seamless computing environment.
Seat management	A support service concept encompassing the management, operation, and maintenance of the services provided by the desktop (computer), portable desktop, servers, communications, printers, peripherals and the associated network components and infrastructure.
SIPRNET	Secret Internet Protocol Router Network. The Department of Defense's IP network supporting the processing and transfer of classified (up to SECRET) information.
SLA	Service Level Agreement - a definition of the type, quality, and quantity of services agreed to by the provider and the customer.
Standard	National and/or International agreement on the rules, procedures, and content of AIS and telecommunications exchanges.
TCP/IP	Transmission Control Protocol/Internet Protocol. A suite of standard protocols or rules for sending and receiving data, addressing, and management information across networks.

GLOSSARY

TCO	Total Cost of Ownership. An assessment method consisting of the cumulative costs associated with the planning, research, prototyping, developing, implementing, operating, maintaining, and disposal of a capital asset.
Thin Client	In the context of this document, "thin client" refers to minimizing the amount of processing logic and data manipulation on a client to the maximum extent possible. The "thinnest" client is nothing more than a terminal. The concept of using thin clients at Post and storing the information in regional data centers is referred to as the "data-less Post" in this document.
TRAG	Technical Review Advisory Group. Chaired by the Deputy Chief Information Officer, this group assesses the technical merits of IT projects, their conformance with IT architectures and standards, and their potential impact on the Department's communications networks and overseas operations
USG	United States Government.
USIA	United States Information Agency – now consolidated in the Department of State.
VPN	Virtual Private Network - a capability to 'split' a physical network or circuit path into two or more sub-paths that use various protocols to define the circuit path and protect the data being transported.
WAN	Wide Area Network. This refers to a collection of circuits that interconnect a widely dispersed set of facilities and other networks - such as a MAN.
Web-based	A system explicitly designed to process its information transaction and exchange requirements using "World Wide Web" conventions such as HTTP and web browsers (end-user applications that display HTTP formatted documents).
X.500	A CCITT protocol, X.500 is a family of standards using a distributed approach to realize a global directory service. Information of an organization is maintained in one or more so-called directory system agendas (DSAs). The X.500 directory supports a variety of services including security (certificates), e-mail (addressing), and "white pages" (name and phone number).
X.509	One of the X.500 standards that defines an electronic security certificate used as a vehicle for associating users with their encryption keys. All of the user's "public" information is stored in an X.509 certificate for use when exchanging information securely with that user. Other information such as to whom does the user belong, what authority issued the keys, when do the keys expire, what levels of information classification is this user allowed to access, and how can the certificate be validated is also included.
Y2K	Year 2000.

This Page Intentionally Left Blank

APPENDIX B

PROGRESS UNDER THE 1997 IRM STRATEGIC AND PERFORMANCE MEASUREMENT PLAN

In the Information Resources Management Strategic and Performance Measurement Plan FY1997-FY2001, issued on January 15, 1997, the Department identified 14 major IRM strategic initiatives it planned to pursue. These initiatives are listed below and are followed by brief summaries of the progress the Department has made on them thus far.

Coordinated Planning and Standards - The Department will strengthen its IRM management processes to coordinate efforts across decentralized organizations.

> *The Department has continued to strengthen its IT management process and has recently instituted a Capital Planning process that meets the requirements of OMB Circular A-11.*

IRM Architecture Standards - The Department's modernization will be standards-based and will emphasize open systems.

> *The Department has issued an Information Technology Architecture and related standards.*

Year 2000 Compliance - The Department will ensure that all IRM systems will operate properly when the Year 2000 is reached.

> *The Department successfully completed Y2K corrections to all of its IT systems, receiving an "A" rating. No significant problems were encountered during the Y2K rollover.*

Information Technology Infrastructure - The Department will establish a modernized information technology infrastructure that satisfies its business requirements.

> *The Department has installed up-to-date unclassified equipment at all of its 270 Foreign Service posts. It has begun to upgrade classified equipment at those posts.*

Global Networking - The Department will implement the three key components of its global network design: ALMA; Bandwidth; and Backbone.

> *The Department has installed unclassified ALMA equipment. It has also installed Backbone facilities in the Main State building and in SA-1.*

Business Quality Messaging - The Department will provide reliable and rapid global classified and unclassified messaging.

> *During the past two years the Department has made major improvements in the speed and reliability of its e-mail systems.*

Voice - The Department will implement a life cycle replacement and enhancement program for its overseas telephone and radio communications.

> *During the past two years the Department has funded telephone systems for 69 overseas posts and radio communications equipment for 293 posts. Additionally, we are implementing a full-scale overseas deployment of a worldwide Emergency and Evacuation Radio network*

Central Processing Facilities - The Department will invest in its central processing facilities, including mainframe and consolidated server-processing centers.

> *The Department has upgraded its central mainframe equipment to support increased border crossing workloads.*

Security - The Department will apply risk management methodologies to minimize inherent risks and meet all appropriate security requirements.

> *The Department has applied risk management methodologies in authorizing implementation of new systems, including CableXpress and the State Archiving System (SAS).*

Desktop Computing Standards - The Department will implement a life-cycle replacement program for desktop computers and software to ensure that knowledge workers have standard and appropriate tools to access information.

> *The Department has installed up-to-date equipment at Foreign Service posts and has begun re-installations to replace components that are now more than four years old.*

Applications and Software Development - The Department will improve its suite of applications and software to meet evolving business requirements.

> *As part of its program to make Y2K corrections, the Department has installed new software systems to support domestic financial management, personnel management, and procurement functions.*

Legacy System and Application Support - The Department will operate legacy systems as modernization proceeds.

> *The Department has continued to operate legacy systems supporting overseas communications and financial management functions. Most other legacy systems have by now been replaced.*

Human Resources Management and Training - The Department will ensure that its workforce is properly skilled, trained and managed.

> *Through the ALMA program the Department has trained more than 10,000 employees in the operation and maintenance of equipment installed at Foreign Service posts.*

Configuration Management & Hardware/Software Maintenance - The Department will require that all projects incorporate CM and maintenance costs into detailed plans according to Department-wide standards and guidelines.

> *The Department has established CM procedures as a by-product of the ALMA program. It also requires project managers to include ongoing maintenance costs in their project management plans.*